



Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

LEONARDO COSTA LIMA SILVA

**UM ESTUDO SOBRE SERVIÇO DE DIRETÓRIO E FERRAMENTAS
DE SEGURANÇA DA INFORMAÇÃO**

Brasília
2015

LEONARDO COSTA LIMA SILVA

**UM ESTUDO SOBRE SERVIÇO DE DIRETÓRIO E FERRAMENTAS
DE SEGURANÇA DA INFORMAÇÃO**

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Redes de Computadores com Ênfase em Segurança da Informação.

Brasília

2015

LEONARDO COSTA LIMA SILVA

**UM ESTUDO SOBRE SERVIÇO DE DIRETÓRIO E FERRAMENTAS
DE SEGURANÇA DA INFORMAÇÃO**

Trabalho apresentado ao Centro
Universitário de Brasília (UnICEUB/ICPD)
como pré-requisito para a obtenção de
Certificado de Conclusão de Curso de
Pós-graduação *Lato Sensu* em Redes de
Computadores com Ênfase em
Segurança da Informação.

.

Brasília, ____ de _____ de 2015.

Banca Examinadora

Prof. Dr.

Prof. Dr. Nome completo

AGRADECIMENTO(S)

Agradeço todo o apoio, compreensão e paciência, em tempos muitos difíceis, a minha namorada Natássia Caroline e ao meu chefe Romulo Rosa.

“Que homem é o homem que não torna o mundo melhor”. Frase retirada do filme Cruzadas.

RESUMO

Este trabalho tem por objetivo abordar o serviço de diretório e a sua importância tanto na operação, manutenção e controle de redes como na segurança dos dados de empresas de todos os portes, bem como mostrar diferentes ferramentas de gerenciamento de diretório, abordando com mais perícia o funcionamento, as diferenças e dificuldades entre ferramentas muito conhecidas no mercado: O Active Directory e o OpenLDAP. Para mostrar as diferenças entre essas ferramentas em termos de segurança, foram usadas, como parâmetro, três regras básicas de segurança conforme padronização internacional ISO 27001, a autenticação de usuários, a administração de políticas de segurança e a segurança no compartilhamento de arquivos, além do próprio processo de instalação e configuração de cada ferramenta. O presente trabalho mostra os detalhes de configuração e de funcionamento dessas ferramentas, concluindo que as ferramentas são eficazes quando testadas, porém a complexidade de configuração e nível de conhecimento necessários para realizar os testes são diferentes, sugerindo que a ferramenta Active Directory é mais amigável, facilitando para o administrador de uma rede realizar sua instalação e configuração com uma interface interativa e acesso fácil à tutorias completos tanto de sítios especializados como do sítio do fabricante. Já a ferramenta de distribuição gratuita, o OpenLDAP, exige conhecimento avançado a nível de linha de comando com interface pouco amigável com acesso a tutoriais diversos de vários sítios para distribuições, o que faz com que muitas vezes seja necessário complementar informações de configuração com aquelas obtidas em fóruns de comunidade de pesquisa.

Palavras-chave: Serviço de Diretório. Active Directory. OpenLDAP. ISO 27001. Segurança.

ABSTRACT

This paper aims to introduce on the directory service and its importance in both the operation, maintenance and network control as well in security of all sizes of enterprises, over all, as showing different directory management tools with more precise focus on the distinct operation, differences and difficulties between two well-known tools on the market, the Active Directory and OpenLDAP. To show the differences between these tools were used as parameter three basic security rules imposed by the international standard ISO 27001, user authentication, administration of security policies and security in file sharing, in addition to the installation process itself and configuration of each tool. This study shows the configuration and operating details of these tools. Concluding that the tools are effective when tested, however the complexity of configuration and level of knowledge required to perform the tests are different, suggesting that the Active Directory tool is more user friendly and interactive, making it easier for the administrator to perform a network installation and configuration, an interactive interface and easy access to complete tutorials from both specialized websites and manufacturer website. Already tool free distribution, OpenLDAP, requires advanced knowledge level of the command line with unfriendly interface with access to numerous tutorials from various sites for various distributions and who are not always applicable, in addition the support is based on forums searches.

Key words: Directory Service. Active Directory. OpenLDAP. ISO 27001. Segurança.

SUMÁRIO

INTRODUÇÃO	10
1 O SURGIMENTO DO SERVIÇO DE DIRETÓRIO	12
1.1 Serviço de Diretório	12
1.1.1 <i>OpenLDAP</i>	13
1.1.2 <i>Edirectory</i>	13
1.1.3 <i>Microsoft Active Directory</i>	14
1.2 Autenticação	14
2 MICROSOFT ACTIVE DIRECTORY	16
2.1 Identidade e Acesso	16
2.2 Domínio do Active Directory	17
2.3 Infraestrutura IDA	18
2.4 Componentes do Active Directory	20
2.4.1 <i>Armazenamento de Dados</i>	21
2.4.2 <i>Controladores de Domínio</i>	21
2.4.3 <i>Unidades Organizacionais</i>	22
2.4.4 <i>Domínio</i>	23
2.4.5 <i>Floresta</i>	23
2.4.6 <i>Árvore</i>	24
2.4.7 <i>Replicação</i>	24
2.4.8 <i>Sites</i>	25
2.4.9 <i>Relação de Confiança</i>	25
3 OpenLDAP	27
3.1 Identidade Única	28
3.2 Entrada LDAP	29
3.3 Árvore de Informações do Diretório	30
3.4 Componentes do OpenLDAP	30
3.4.1 <i>Servidores</i>	31
3.4.2 <i>Clientes</i>	32
3.4.3 <i>Utilitários</i>	32
3.4.4 <i>Bibliotecas</i>	32
4 ISO 27001	33
4.1 Objetivos de Controle	34

4.2 Objetivos de Controle Aplicados aos Sistemas de Serviço de Diretório	35
5 ISO 27001 APLICADA AO ACTIVE DIRECTORY E AO OPENLDAP EM AMBIENTE DE TESTE PARA FINS COMPARATIVOS EM PARAMETROS EQUIPARADOS	37
5.1 Testes com o Microsoft Active Directory	37
5.1.1 <i>Configurar IP Estático</i>	37
5.1.2 <i>Verificação do Nome do Servidor</i>	40
5.1.3 <i>Instalação do Serviço de Diretório</i>	41
5.1.4 <i>Desafio ao Active Directory</i>	56
5.1.5 <i>Criação de Usuários</i>	56
5.1.6 <i>Criação dos Grupos</i>	58
5.1.7 <i>Inclusão de Servidores e Clientes no Domínio</i>	61
5.1.8 <i>Experimento 1 – Criação de Políticas de Segurança e Verificação dos resultados</i>	67
5.1.8.1 <i>Editar</i>	73
5.1.8.2 <i>Verificar a Política Aplicada</i>	76
5.1.9 <i>Experimento 2 – Criação de Política de Acesso em Pastas de Servidor de Arquivos e Verificar os Resultados</i>	81
5.1.9.1 <i>Criação de Pastas no Servidor de Arquivos</i>	81
5.1.9.2 <i>Criação da Política de Acesso às Pastas de Armazenamento de Arquivos</i>	82
5.1.9.3 <i>Verificação da Eficácia da Política de Acesso as Pastas</i>	85
5.2 Testes com o OpenLDAP	88
5.2.1 <i>Criar um domínio com um banco de usuários</i>	91
5.2.2 <i>Por que SAMBA?</i>	93
5.2.3 <i>Testes Samba</i>	94
5.2.3.1 <i>Instalação do Ubuntu Server 14.04</i>	94
5.2.3.2 <i>Configuração do Controlador de Domínio</i>	108
5.2.3.3 <i>Configurar IP Estático</i>	110
5.2.3.4 <i>Modificar o Nome do Computador</i>	112
5.2.3.5 <i>Atualizar o Sistema</i>	114
5.2.3.6 <i>Pré-requisitos</i>	115
5.2.3.7 <i>Instalação do SAMBA</i>	118

5.2.3.8 Criação do Domínio.....	120
5.2.3.9 Configuração do DNS.....	121
5.2.3.10 Configurar o Kerberos.....	123
5.2.3.11 Pastas para Usuários.....	126
5.2.3.12 Senha de Administrador.....	128
5.2.3.13 Configurar IP da Máquina Cliente.....	129
5.2.3.14 Adicionar Computador Cliente no Domínio.....	133
5.2.3.15 Instalar as Ferramentas de Gerencia do Domínio.....	136
5.2.3.16 Autenticação no Domínio.....	141
CONCLUSÃO	150
REFERÊNCIAS	152

INTRODUÇÃO

É possível observar que ferramentas básicas de segurança de tecnologia da informação nos dias de hoje são montadas sobre sistemas de diretório. Os sistemas de diretório armazenam informações de pessoas, objetos ou qualquer matéria que possa ser catalogada em um banco de dados que permita consulta a qualquer momento. Porém, a consulta às informações armazenadas no banco de diretórios podem ser controladas de várias formas, com ferramentas distintas. Essas ferramentas garantem a segurança da informação.

O presente estudo apresenta uma introdução aos serviços de diretório e às ferramentas de gerenciamento de serviços de diretório Microsoft Active Directory e OpenLDAP para Linux. Propõe uma comparação de esforço e acesso ao conhecimento para instalar e configurar sistemas de diretório com uma segurança baseada na ISO 27001, utilizando ambiente virtualizado.

O objetivo do presente trabalho é comparar duas ferramentas muito utilizadas de gerenciamento de diretório, no caso o Active Directory e OpenLDAP, capazes de aplicar segurança de acesso a informação nos quesitos: praticidade, compatibilidade, esforço, acesso ao conhecimento, eficácia e eficiência, além de, mostrar uma configuração possível em laboratório onde o Linux e o Windows coexistem em um ambiente com serviço de diretório.

Para alcançar esse objetivo, procedeu-se da seguinte maneira, foi feita a instalação dos sistemas operacionais Windows Server e Ubuntu Server, ambos capazes de suportar o Active Directory e o OpenLDAP respectivamente. Em seguida a instalação e configuração do Active Directory e do OpenLDAP com os serviços de autenticação e controle de usuário a partir de um domínio, aplicação de política de segurança quanto à complexidade de senhas e o compartilhamento com controle de acesso a arquivos e pastas. Um servidor Linux foi montado como servidor de diretórios e uma máquina Windows como interface gráfica para manipulação do diretório.

Espera-se demonstrar com este estudo a importância da segurança aplicada ao serviço de diretório e principalmente a formação de opinião quanto às necessidades em torno das ferramentas apresentadas neste trabalho e ainda

apresentar uma solução para que essas ferramentas coexistam para funcionamento de um serviço de diretório.

O presente trabalho foi então estruturado em 5 capítulos, como a seguir.

No primeiro capítulo, apresentam-se uma introdução ao sistema de diretório. O que é, para que serve e como funciona alguns tipos de gerenciadores de sistemas de diretório. O segundo capítulo é focado no funcionamento do básico do Microsoft Active Directory. O terceiro capítulo, apresenta o foco no gerente de sistema de diretório OpenLDAP. No quarto é apresentado a ISO 27001 e os parâmetros nela contidos que serão usados nos testes dos programas. O quinto e último capítulo é apresentado como foram feitos os testes com as duas ferramentas nas mesmas condições de ambiente com os mesmos parâmetros de segurança além da solução para coexistência das ferramentas.

1 O SURGIMENTO DO SERVIÇO DE DIRETÓRIO

Sabemos que no início da humanidade a comunicação era limitada somente a gestos e grunhidos. Com o crescimento da humanidade a comunicação sofreu vários avanços ganhando forma e sofisticação. Fica perceptível que com o passar dos anos a comunicação passou a ter um valor comercial, dependendo do seu conteúdo. Cada Informação trocada passou a ter um grau importância.

Na época em que começaram a haver guerras por exemplo, a informação passada entre os comandantes precisava ser protegida. E muitos morreram para proteger esse tipo de informação por tentar protegê-la.

Após o advento do micro computador percebeu-se a necessidade de continuar protegendo a informação, principalmente com o surgimento das redes de comunicação de computadores.

Em 1967 a primeira rede de comunicação de computadores de diferentes fabricantes estava pronta. Através de um IMP (*Interface Message Processor*), máquina ao qual vários computadores eram interligados, foi feita a comunicação entre máquinas de diferentes fabricantes por meio de tradução. (FOROUZAN; FEGAN, 2008).

Quando computadores passaram a ter acesso a outros computadores foi preciso fazer planos para proteger a informação: políticas de segurança; antivírus; departamentos de segurança da informação; entre outros.

Foi a partir dessa ideia de controle de acesso a informação que várias corporações que primam por segurança da informação desenvolveram sistemas para controlar esse acesso, entre esses sistemas está o sistema de serviço de diretório.

1.1 Serviço de Diretório

O serviço de diretório de rede é um serviço que gerencia objetos de uma rede de forma a fazer o controle de acessibilidade, protocolos de comunicação,

certificação digital entre outros, em recursos da rede como usuários, computadores, pastas, documentos e aplicações utilizando o método de autenticação. Alguns conceituam o serviço de diretório como sendo apenas uma comparação com o serviço prestado por uma lista telefônica que armazena dados para busca. No entanto o serviço de diretório engloba tanto o armazenamento de informações como o gerenciamento das mesmas através de ações específicas.

Hoje no mercado, as aplicações de serviço de diretório que estão entre as mais conhecidas e implantadas são: (MARINHO, 2013)

- *OpenLdap* para sistemas *open source*;
- *Edirectory* para sistemas Novell;
- *Active Directory* para sistemas *Microsoft* com suporte aos acima citados.

1.1.1 *OpenLDAP*

O *Open Ldap (Lightweight Directory Access Protocol)* é um serviço de diretório aberto, ou seja, seu código fonte pode ser modificado, permitindo dessa forma a incorporação completa de serviços que são realizados por sistemas operacionais de rede. É bastante utilizada em plataforma Linux para construção de serviços de diretório distribuídos. Em comparação com outras soluções de diretórios, o *Open Ldap* apresenta um bom grau de tolerância a falhas e bom desempenho. (RIBEIRO et al., 2004)

1.1.2 *Edirectory*

O *Edirectory* foi desenvolvido pela Novell, que criou um serviço de diretório *standalone* e *cross-plataform* para suportar *e-commerce*, relacionamento B2B e aplicações em *internet*, também trabalhando com o *FSD (Full Service Directory)*, um banco de dados genérico que gerencia busca, descoberta,

segurança, armazenamento e relacionamentos de objetos. (SHERESH; SHERESH, 2002)

1.1.3 Microsoft Active Directory

O *Active Directory* (AD) é o sistema operacional de diretório de rede da *Microsoft*, construído sobre o *Windows 2000* e o *Windows Server 2003*. Esse sistema operacional habilita administradores de redes gerenciar quase toda a informação da rede eficientemente de um repositório central que pode ser globalmente distribuído. Uma vez que informações sobre usuários e grupos, computadores e impressoras, aplicações e serviços são adicionadas ao *Active Directory* também se tornam disponíveis para uso em toda a rede para todos os objetos da rede que os administradores do sistema derem autorização de acesso. (RICHARDS et al., 2006)

1.2 Autenticação

Em sua essência autenticação significa o que o próprio nome diz, processo de verificação de autenticidade. O processo da autenticação é encontrado em praticamente todos os serviços de diretório. Mas o propósito principal de se ter o um processo de autenticação em um serviço de diretório é de verificar se objetos que estão fora de uma rede pertencem ou não aquela rede e se devem ou não ter acesso a outros objetos dentro da mesma. A autenticação é feita quase da mesma forma na maioria dos serviços de diretório.

Existem dois tipos de autenticação:

- Local ou interativa: O usuário faz uma autenticação diretamente a um computador, assim como quando é feito o acesso a um *laptop*.
- Remoto ou de rede: O usuário que está em seu laptop faz uma autenticação em outro computador para ter acesso a outros

recursos da rede como em um servidor de arquivos ou de email para acessar recursos específicos dos mesmos.

2 MICROSOFT ACTIVE DIRECTORY

Faz parte do trabalho de um profissional de TI, conectar usuários de uma rede com a informação necessária para que eles façam seu trabalho. Devido aos usuários precisarem de diferentes níveis de acesso e diferentes classes de informação é preciso associar o usuário correto à um nível de acesso específico para proteger a informação.

Existem várias formas de proteger e classificar uma informação:

- **Identidade e Acesso (IDA):** Usuários e outros ativos de segurança, que pode incluir também computadores, serviços e grupos são chamados de identidades ou contas aos quais é dado acesso (permissões) a informações, recursos, ou sistemas.
- **Autenticação, Autorização, Identificação (AAA):** Usuários fornecem um nome de usuário e uma senha que são autenticadas quando suas credenciais são validas. Os usuários recebem permissões (controle de acesso) que são usados para autorizar as requisições de acesso. O acesso é monitorado, provendo identificação de audição.
- **Confidencialidade, Integridade e Disponibilidade (CIA):** A informação é protegida para garantir que não é acessível para usuários não autorizados (confidencialidade), não é modificada incorretamente (integridade) intencionalmente ou acidentalmente, e disponível sempre que necessário (disponibilidade).

2.1 Identidade e Acesso

O Active Directory é o serviço de diretório fabricado pela Microsoft e feito para funcionar em um ambiente de redes com Windows. Em um sistema protegido cada usuário é representado por um uma identificação. Nos sistemas Windows, a identidade é a conta do usuário. As contas de um ou mais usuários são colocadas em um armazenamento de identidades, que também é conhecido como banco de

dados de diretório. Uma identidade é chamada de objeto de segurança nos sistemas Windows. Os objetos de segurança são unicamente identificados por um atributo chamado de identidade de segurança (SID).

Do outro lado do sistema está o recurso o qual o usuário requer acesso. O recurso está segurado com permissões, e cada permissão tem um nível de acesso específico. Muitos recursos do Windows são segurados por um descritor de segurança que contém uma lista de controle de acesso discricionária (DACL) em que cada permissão tem a forma de uma entrada de controle de acesso (ACE).

O sistema tem um funcionamento simples, é preciso apenas mapear o SID de um usuário a seu ACE apropriado de um recurso. (MICROSOFT, 2011)

2.2 Domínio do Active Directory

Quando um usuário precisa fazer acesso a sua máquina ele é questionado quanto suas credencias armazenadas dentro computador. Cada computador mantém somente um único armazenamento confiável: uma lista local de usuários e grupos armazenados em um registro, o banco de dados Gerente de Contas de Segurança (SAM).

Se o usuário precisar acessar uma pasta compartilhada em um servidor através de seu computador, não será bem sucedido. Isso devido a que cada computador confia no seu próprio banco de credencias SAM. Se por acaso o usuário tiver suas credencias catalogadas no SAM do servidor em que se encontra a pasta compartilhada identicamente às credenciais do SAM em seu computador, o acesso será permitido sem problemas. Mas se alguém trocar qualquer detalhe nas credenciais tanto do servidor como do computador do usuário, as credencias do SAM das duas maquinas não estarão mais sincronizadas, por tanto não será possível fazer o acesso conforme desejado. Se mais usuários forem adicionados no SAM dos servidores de pastas compartilhadas a probabilidade de algum usuário não estar sincronizado é muito grande.

Para resolver esse problema a Microsoft criou um SAM centralizado, onde nenhum usuário precisa ter um cadastro idêntico em cada computador da rede, mas

sim cada usuário tem apenas um cadastro em um banco de identidades confiável para todos os computadores. Esse banco de credenciais centralizado faz parte da infraestrutura de domínio e florestas do Active Directory.

Um domínio do Active Directory provê um armazenamento de identidades centralizado e confiável para todos os computadores que fazem parte do domínio. Um domínio também fornece um serviço de autenticação centralizada. Tanto o armazenamento de identidades como os serviços de autenticação centralizados, junto com outros serviços e componentes, são armazenados em um servidor fazendo o papel de um controlador de domínio.

2.3 Infraestrutura IDA

Uma infraestrutura de identidade de acesso ou IDA é necessária para manter a segurança de recursos de uma empresa como arquivos, e-mails, aplicações e banco de dados. Seu funcionamento se caracteriza da seguinte forma:

- Armazenar informações de usuários, grupos, computadores e outras identidades. Uma identidade é uma representação de uma entidade que tomará ações dentro de uma rede empresarial. Por exemplo um usuário abre documentos dentro de uma pasta compartilhada. Quando esse usuário acessa um documento dentro da rede ele passará por uma lista de controle de acesso ou ACL. O acesso a documentos dentro da rede é gerenciado pelo subsistema de segurança do servidor que compara a identidade do usuário com as identidades dentro da ACL para determinar se a solicitação do usuário de acessar o documento é permitida ou negada. Computadores, grupos, serviços e outros objetos também têm uma identificação. Junto com cada identificação de objeto estão as propriedades desse objeto formando uma identificação única, como um nome de usuário ou um SID e o password da identidade. O armazenamento de identidades é um componente da infraestrutura IDA. O armazenamento de dados do Active Directory também conhecido como diretório é um armazenamento

de identidades. O diretório é localizado dentro de um controlador de domínio, um servidor fazendo papel de AD DS, que também faz seu gerenciamento.

- Autenticar uma identidade. O servidor não vai assegurar acesso a um usuário a não ser que o servidor verifique que a identidade apresentada na solicitação de acesso seja válida. Para validar a identidade o usuário fornece um segredo apenas conhecido pelo próprio usuário e pela infraestrutura IDA. Esses segredos são comparados com a informação no armazenamento de identidades em processo chamado de autenticação.
- Em domínio do Active Directory, um protocolo chamado Kerberos é usado para autenticar identidades. Quando um usuário ou um computador faz um *login* (acesso) no domínio, o Kerberos autentica as credenciais e verifica um pacote de informações chamado TGT (ticket granting ticket). Antes do usuário se conectar ao servidor para requisitar um documento, uma solicitação Kerberos é enviada para o controlador de domínio junto com o TGT que serve para identificar o usuário autenticado. O controlador de domínio verifica outro pacote de informação do usuário chamado ticket de serviço que identifica o usuário autenticado ao servidor. O usuário apresenta o ticket de serviço ao servidor, que aceita o ticket de serviço como prova que o usuário foi autenticado.
- Essas transações Kerberos resultam em um acesso único na rede ou *single sign-on*. Após o usuário ou computador ter inicialmente acessado a rede e tenha coletado um TGT, o usuário está autenticado dentro de todo o domínio e pode estar conseguindo tickets de serviço que identificam o usuário a qualquer serviço. Toda essa atividade com tickets é gerenciada pelos clientes Kerberos e serviços construídos no Windows, é transparente para o usuário.

- Controle de acesso. A infraestrutura IDA é responsável por proteger informações confidenciais como informações armazenadas em um documento. Acesso a documentos confidenciais precisam ser gerenciados de acordo com as políticas de segurança da empresa. Uma ACL para um documento reflete uma política de segurança que contém permissões que especificam níveis de acesso a identidades específicas. O subsistema do servidor neste exemplo está realizando a funcionalidade de controle de acesso em uma infraestrutura IDA.
- Prover uma trilha de auditoria. Uma empresa deve querer monitorar as mudanças e atividades dentro da infraestrutura IDA, então é preciso fornecer um mecanismo para gerenciar auditoria.

2.4 Componentes do Active Directory

Abaixo estão os componentes que estão entre os principais do Active Directory:

- Armazenamento de Dados;
- Controladores de Domínio;
- Unidades Organizacionais;
- Domínio;
- Floresta;
- Arvore;
- Replicação;
- Sites;
- Relações de Confiança.

2.4.1 Armazenamento de Dados

O serviço de domínio do *Active Directory* armazena as identidades em um diretório que fica dentro de um controlador de domínio. O diretório é um arquivo único chamado de `ntds.dit`, e seu local padrão é na pasta `%systemroot%\ntds` dentro de um controlador de domínio.

O banco de dados é dividido em algumas partições:

- **Schema:** Define o atributo e os tipos dos objetos que podem ser armazenados no diretório.
- **Contexto de Nomeação do Domínio (NC do Domínio):** Contém dados sobre os objetos do domínio como, usuários, grupos e computadores. Quando é feita uma alteração no índice usuários e computadores do Active Directory, como adicionar um usuário ou computador, o conteúdo do NC do domínio é modificado.
- **Configuração:** Contém informações sobre domínios, serviços e topologia.
- **DNS:** Contém informações e recursos do DNS.
- **Configuração de Atributos Parcial (PAS):** É a partição usada pelo catálogo global.

O Active Directory também armazena informações em uma pasta chamada `SYSVOL`. Por padrão esta pasta é localizada em `%systemroot%\SYSVOL`. Contém itens como *scripts* de *logon* e arquivos relacionados a políticas de grupo (GPOs). (MICROSOFT, 2011)

2.4.2 Controladores de Domínio

Controladores de domínio também conhecidos como DCs tem a função de serviço de domínio. Parte dessa função dessa função é reter e replicar o banco de dados do Active Directory (NTDS.DIT) e `SYSVOL`.

Os DCs também executam o Centro de Distribuição de Chaves Kerberos (KDC) que realiza autenticação e outros serviços do Active Directory.

Devido a autenticação ser crítica para uma empresa a melhor pratica é sempre ter a disposição dois DCs, pois se usuários tiverem problemas de acesso a um deles podem ser autenticas no outro disponível. (MICROSOFT, 2011)

2.4.3 Unidades Organizacionais

Uma unidade organizacional (OU) é um objeto do serviço de domínio do AD (AD DS) dentro do domínio que pode ser usado para tarefas específicas como:

- Organizar objetos dentro de um domínio. OUs contém objetos do domínio, como contas de usuários e computadores, e grupos. Compartilhamento de arquivos e impressoras que são publicados para o AD DS também são encontrados nas OUs.
- Delegar controle administrativo. Pode-se designar até controle administrativo completo, como a permissão de controle total, sobre todos os objetos na OU ou designar controle administrativo limitado, como a habilidade de modificar informações de email de objetos dentro da OU. Para delegar controle administrativo é preciso designar permissões específicas em uma OU e objetos que estão contidos na OU para um ou mais usuários e grupos.
- Simplificar o gerenciamento de recursos agrupados comumente. Usando OUs, podem-se criar containers que representam estruturas lógicas ou hierárquicas, na organização. Desta forma pode-se usar uma política de grupo para gerenciar a configuração das definições de usuário e computador baseado no modelo organizacional da empresa.

2.4.4 Domínio

Um ou mais controladores de domínio são necessários para criar um domínio do Active Directory. Um domínio é uma unidade administrativa onde certas capacidades e características são compartilhadas. Todos os controladores de domínio replicam a partição de armazenamento de dados do domínio, que contém, entre outras coisas, os dados de identidade dos usuários, grupos, e computadores do domínio. Desta forma todas os DCs mantem o mesmo armazenamento de identidade, ou seja, qualquer DC pode realizar a autenticação de uma identidade no domínio.

Um domínio é um escopo de políticas administrativas como complexidade de senha e políticas de bloqueio de senha. Essas políticas que são configuradas no domínio afetam todas as contas do domínio e não afetam as contas de outro domínio. (MICROSOFT, 2011)

2.4.5 Floresta

Uma floresta é uma coleção de um ou mais domínios do Active Directory. O primeiro domínio instalado em uma árvore é chamado de domínio raiz da floresta. Uma floresta tem uma definição única da configuração da rede e uma única instancia do schema do diretório. Cada controlador de domínio na floresta replica a partição da configuração e do schema, e essas duas partições são as mesmas para cada domínio da floresta, ou seja, não se pode ter mais de uma configuração e um schema em uma floresta. O domínio raiz da floresta contém contas administrativas de toda a floresta como a Enterprise Admin e Schema Admin. A conta Enterprise Admin tem privilégios administrativos em todos os domínios da floresta, podendo editar a estrutura da floresta adicionando ou removendo domínios, estendendo schema entre outros.

Uma floresta é uma instancia única no diretório, nenhuma informação do diretório é replicada para fora das barreiras da árvore. Porém a floresta define os limites de replicação e segurança. (MICROSOFT, 2011)

2.4.6 Árvore

A configuração de nome do Domain Name System (DNS) do domínio dentro de uma floresta pode criar árvores. Se um domínio é um subdomínio de outro domínio, esses domínios são considerados juntos uma árvore. Por exemplo se a floresta trayresearch.net contém dois domínios traysearch.net e antártica.traysearch.net, os domínios constituem uma porção contígua da configuração de nome do DNS portanto são considerados uma árvore. Se por ventura houver mais um domínio chamado proseware.com, que não é contíguo aos outros dois domínios então tem-se duas árvores na floresta. As árvores são resultados diretos dos nomes DNS escolhidos para os domínios em uma floresta.

2.4.7 Replicação

Os Serviços de replicação distribuem dados do diretório por toda a rede. Isso inclui armazenamento de dados e dados requeridos para implementar políticas e configuração, incluindo *scripts* de *logon*. O Active Directory tem uma partição separada dos dados armazenados chamados de configuração, que tem informações sobre a configuração da rede, a topologia e serviços.

O Active Directory também usa uma replicação multimaster para sincronizar as informações do diretório. A verdadeira replicação multimaster pode ser contrastada com outros serviços de diretório que utilizam a abordagem mestre-escravo para as atualizações onde todas as atualizações precisam ser feitas no mestre depois copiadas para os escravos. A abordagem mestre-escravo é adequada para organizações com um número pequeno de cópias e onde as modificações podem ser feitas centralizadamente. No Active Directory nenhum DC é um mestre, ao invés disso, todos os DCs dentro de um domínio são equivalentes. Mudanças podem ser feitas em um DC que todos os outros serão sincronizados periodicamente.

Na replicação multimaster não é necessário replicar para cada DC, o sistema implementa um robusto conjunto de conexões que determina que DC deve sincronizar informações com que outro DC. Isso garante que a rede não ficará sobrecarregada com tráfego de replicações desta forma a latência de replicações não fica longa de forma a causar inconveniência a usuários. O conjunto de conexões por onde as modificações são replicadas para os DCs dentro de uma empresa é chamada de topologia de replicação. (MICROSOFT, 2011)

2.4.8 Sites

No Active Directory os sítios ou *sites* têm um significado específico devido a uma classe de objeto específica no AD chamada *site*.

Um site do Active Directory é um objeto que representa uma porção da empresa onde a conectividade de rede é boa. Um site cria um limite de replicação e utilização de serviços. Também é considerado uma interpretação lógica da rede física.

Controladores de domínio replicam mudanças dentro de um site em segundos. Mudanças são replicadas entre sites em uma base controlada assumindo que as conexões entre sites são lentas, caras ou não confiáveis. Ao criar um site é o mesmo que dizer ao Active Directory que existem vários controladores de domínio em lugares físicos na rede e que a conexão entre esses lugares é lenta. (MICROSOFT, 2011)

2.4.9 Relação de Confiança

Para um novo computador ser adicionado no domínio do Active Directory primeiro é preciso ter um usuário confiável, ou seja que tenha suas credenciais armazenadas no banco de dados do domínio, uma vez que esse usuário é autenticado no domínio estabelece-se uma relação de confiança entre o novo computador adicionado e o AD.

O mesmo conceito pode ser estendido entre domínios. Um domínio pode autenticar usuários de outro domínio e ter permissão para esses usuários acessarem recursos do outro domínio. Isso é possível quando se estabelece uma relação de confiança entre domínios. (MICROSOFT, 2011)

3 OPENLDAP

OpenLDAP é um programa que utiliza o protocolo LDAP (*Lightweight Directory Access Protocol*) para fazer centralização de autenticação e banco de dados oferecendo um serviço de diretório.

O modelo geral do protocolo LDAP baseia-se em operações de protocolo realizadas entre um cliente e um servidor. Neste modelo, o cliente transmite uma solicitação de protocolo descrevendo a operação que será feita para um servidor. O servidor então é o responsável por realizar as operações necessárias no diretório. Uma vez completada as operações, o servidor então retorna uma resposta contendo o resultado ou erro ao cliente solicitante. (RFC 2251)

O protocolo LDAP é padronizado e assim como protocolos de rede, a estrutura de diretório e serviços providos por um servidor LDAP estão todos disponíveis em RFCs (*Requests for Comments*).

A versão mais atual do LDAP é a v.3 (versão 3), um padrão desenvolvido em 1997 na RFC 2251. A especificação original foi atualizada em 2006, e RFCs de 4510 a 4519 fornecem especificações mais claras e coesivas para o LDAP.

Alguns tipos de serviços de diretório apenas fornecem um serviço limitado e específico. Um servidor de diretório com propósito único, assim com um dicionário de endereços, deve armazenar apenas um tipo específico de dado, como números de telefone, endereços e informações de *e-mail* de algumas pessoas. Esses tipos de diretórios não são extensíveis, apenas tem um propósito único.

O LDAP foi desenvolvido para ser servidor de diretório com propósito geral ou seja, foi desenvolvido para que os administradores dos servidores possam definir que tipo de informação deve ser armazenado pelo servidor, com clareza e cuidado.

Um diretório genérico permite armazenar muitos tipos de informação, desta forma deve armazenar muitos tipos de informação sobre vários diferentes tipos de entidades. Por exemplo, um diretório de propósito geral deve armazenar informações sobre entidades como pessoas além de informações sobre amostras de

pedras por exemplo. Mas as informações que serão armazenadas de pessoas não são as mesmas que seriam armazenadas sobre pedras.

Uma pessoa deve ter um nome de usuário, um telefone ou um e-mail, já uma pedra deve ter um número de identificação, informações sobre sua origem geográfica ou sua classificação de solidez.

O protocolo LDAP torna possível definir como uma entrada sobre pessoas deve parecer e como uma entrada sobre rochas deve parecer. Essa arquitetura geral fornece as capacidades necessárias para o gerenciamento de grandes quantidades de diversas entradas de diretório.

3.1 Identidade Única

A melhor forma de distinguir entre duas entradas muito similares é criar uma identidade única para cada entrada, cada dado, armazenado no diretório. Essa é a estratégia adotada pelo LDAP. Cada entrada de armazenamento no diretório tem um *distinguished name* (nome distinguido) abreviado como DN.

Em um diretório LDAP, o criador do diretório é quem decide que componentes vão fazer parte do DN, mas tipicamente o DN reflete à sua localidade dentro do diretório, assim como algumas informações que distinguem essa entrada das outras semelhantes.

Uma DN então, é composta de uma combinação de informação de diretório por exemplo:

```
dn: o=Acme Services, l=Chicago, st=Illinois,
c=US (BUTCHER, 2007)
```

Este único identificador é suficiente para distinguir entre uma empresa da cidade de *Springfield* com o mesmo nome. A DN da empresa de *Springfield* seguindo o mesmo raciocínio seria:

```
dn: o=Acme Services, l=Springfield,
st=Illinois, c=US (BUTCHER, 2007)
```

Quando definindo que campos farão parte da DN, é necessário ter certeza de que os campos escolhidos serão suficientes para separar e distinguir entre duas diferentes entradas. Em outras palavras tudo que é preciso para quebrar a sintaxe da DN criada para o exemplo, é o surgimento de outra empresa, chamada *Acme Services* em Chicago.

3.2 Entrada LDAP

Uma entrada LDAP ou uma gravação LDAP, é a unidade do diretório que armazena a informação sobre um item individual dentro do diretório e essa entrada contém informações sobre uma unidade específica porem o alvo exato dessa unidades não é específico. Pode ser uma pessoa, uma rocha, uma empresa ou alguma entidade virtual como um objeto Java.

Uma entrada LDAP é composta de um DN e um ou mais atributos. O DN serve como um identificador único dentro da árvore de informação do diretório LDAP. Os atributos fornecem informações sobre a entrada.

```
dn: o=Acme Services, l=Chicago, st=Illinois,
c=US
```

```
o: Acme Services
```

```
postalAddress: 123 West First Street
```

```
l: Chicago
```

```
st: Illinois
```

```
postalCode: 60616-1234
```

```
c: US
```

```
telephoneNumber: +1 773 555 8943
```

```
telephoneNumber: +1 800 555 9834
```

```
objectclass: organization (BUTCHER, 2007)
```

A primeira linha é o DN e as outras linhas representam os atributos. Esse é um formato de entrada simples que será interpretada pelo diretório.

Existem muitas variações e regras que diferenciam um atributo do outro e essas regras são gravadas dentro de um *schema* (esquema) compacto, que o servidor de diretório mantém armazenado para consulta.

Os atributos não são sensíveis a caixa alta ou baixa. O atributo com nome *o* é tratado como sinônimo com nome *O*. Assim como, *GivenName*, *givenname* e *givenName* são todos avaliados como sendo o nome do mesmo atributo.

3.3 Árvore de Informações do Diretório

A informação em um diretório telefônico é tipicamente armazenado em uma lista alfabética. A informação em um diretório LDAP é organizado em uma ou mais hierarquias, onde no topo da hierarquia, existe uma entrada base e as outras entradas são organizadas abaixo como uma árvore que tem como base a entrada base. Cada nó na hierarquia é uma entrada, com uma DN e mais de um atributos.

Essa coleção de entradas organizadas hierarquicamente é chamada de Árvore de Informações do Diretório, também sendo referido como Árvore do Diretório ou DIT (*Directory Information Tree*).

Aplicações de dentro de uma organização podem fazer conexão com o diretório LDAP, autenticando seus usuários no diretório.

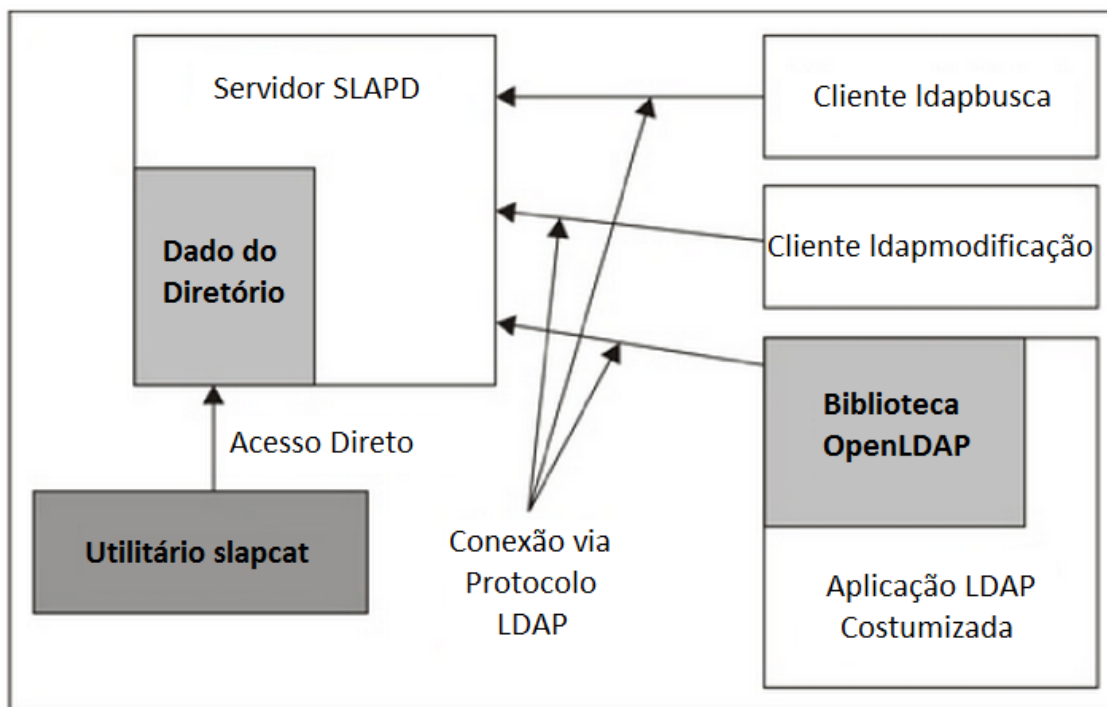
3.4 Componentes do OpenLDAP

O pacote Open LDAP é composto por quatro componentes principais:

- Servidores: Fornecem os serviços LDAP;
- Clientes: Manipulam os dados LDAP;
- Utilitários: Servidores LDAP de suporte;
- Bibliotecas: Fornecem interfaces de programação para o LDAP.

Esses quatro componentes funcionam conforme a figura 1 abaixo:

Figura 1 – Comunicação dos componentes do Open LDAP



Fonte - Adaptado de Butcher (2007)

3.4.1 Servidores

O Servidor principal do pacote LDAP é SLAPD (Stand-Alone LDAP Daemon). Este servidor fornece acesso a uma ou mais árvores de diretório. Os clientes conectam-se ao servidor através do protocolo LDAP, normalmente usando conexão de rede.

Um servidor pode armazenar dados de diretório localmente, ou acesso simples (ou acesso proxy) a fontes externas. Tipicamente, fornece autenticação e serviços de busca e também pode suportar adição, remoção e modificação de dados do diretório. Isso fornece controle de acesso ao diretório.

3.4.2 Clientes

Clientes acessam os servidores LDAP através do protocolo de rede LDAP. Seu funcionamento se caracteriza por requisitar que o servidor realize operações específicas. Tipicamente o cliente primeiro irá se conectar ao servidor de diretório, fazer autenticação e então realizar nenhuma ou alguma operação (pesquisa, modificação, adição, deleção, assim por diante), fazer a operação reversa da autenticação e desconectar.

3.4.3 Utilitários

Ao contrário dos clientes, os utilitários não realizam operações usando o protocolo LDAP. Os dados são manipulados em camadas mais baixas e sem mediação pelo servidor. São usados principalmente para manutenção do servidor.

3.4.4 Bibliotecas

Existem várias bibliotecas *Open LDAP* que são compartilhadas entre aplicações LDAP. As bibliotecas fornecem funções LDAP para essas aplicações. Os clientes, utilitários e servidores compartilham acesso a algumas dessas bibliotecas.

Interfaces de Programação de Aplicação (APIs) são fornecidas para permitir que desenvolvedores de *software* escrevam suas próprias aplicações LDAP sem ter que reescrever o código fundamental LDAP.

Enquanto as APIs fornecidas com o Open LDAP são escritas em C, o projeto do Open LDAP também possui duas APIs Java. Essas bibliotecas em Java não são incluídas no pacote do OpenLDAP. Mas essas APIs podem ser encontradas no site da aplicação (www.openldap.org).

4 ISO 27001

A partir do momento em que se deve proteger um sistema de informações é preciso que se estabeleça um conjunto de regras para acesso e distribuição da informação. Setores específicos tem acesso apenas aos documentos que lhes têm interesse, o funcionário não deve explicitar a sua senha de acesso, a senha de acesso deve ter um nível de complexidade que dificulte quem tentar adivinhar essas senhas, ou seja, um conjunto de regras criadas para garantir a segurança da informação e esse conjunto de regras também é conhecido como política de segurança da informação.

Porém, para a construção de uma política de segurança é preciso seguir algumas normas de segurança padronizadas, que são definidas pela ISO (International Organization for Standardization).

A ISO responsável por padronizar a segurança da informação é a 27001.

A ISO 27001 adota um modelo de controle para criação, implantação e verificação de normas de segurança de informação, o PDCA (*Plan-Do-Check-Act*), é utilizado para estruturar todos os processos do Sistema de Gestão de Segurança da Informação (SGSI). (ISO 27001)

Quadro 1 – Modelo PDCA aplicado aos processos do SGSI

Plan (planejar) (estabelecer o SGSI)	Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
Do (fazer) (implementar e operar o SGSI)	Implementar e operar a política, controles, processos e procedimentos do SGSI.
Check (checar) (monitorar e analisar criticamente o SGSI)	Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.
Act (agir) (manter e melhorar o SGSI)	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Fonte- ISO 27001

4.1 Objetivos de Controle

Os objetivos de controle são aqueles que estão listados no anexo A da ISO 27001 para definir especificidades que devem ser asseguradas com a norma para determinados objetos de tecnologia da informação.

A primeira parte da ISO 27001 explica como as partes atuantes dentro de uma empresa devem se portar e ações que devem ser tomadas por cada parte para que um planejamento estratégico seja aplicado.

O anexo A contém tópicos que especificam detalhes de como uma ação deve ser tomada para um determinado objetivo de controle, por exemplo, o tópico Política de Segurança está definido com o seguinte objetivo:

- Prover uma orientação e apoio da direção para segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Após a definição do objetivo de controle ser definido para a política de segurança da informação, subtópicos apresentam objetos que são relacionados ao objetivo de controle e como realizar o controle sobre ele. Por exemplo, a política de segurança precisa de uma documentação, essa documentação deve ser tratada conforme controle estabelecido nesse subtópico.

- Um documento de política de segurança da informação deve ser aprovado pela direção, publicada e comunicada para todos os funcionários e partes externas relevantes.

O quadro abaixo exemplifica a organização da ISO 27001.

Quadro 2 – Objetivos de controle e controles.

A.5 Política de segurança		
A.5.1 Política de segurança da informação		
<i>Objetivo:</i> Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.		
A.5.1.1	Documento da política de segurança da informação	<i>Controle</i> Um documento da política de segurança da informação deve ser aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.
A.5.1.2	Análise crítica da política de segurança da informação	<i>Controle</i> A política de segurança da informação deve ser analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

4.2 Objetivos de Controle Aplicados aos Sistemas de Serviço de Diretório

Para fazer os testes com os sistemas de serviço de diretório e então compara-los, foram escolhidos objetivos da ISO 27001 que são normalmente adotados em políticas de segurança da informação, são eles, a autenticação de usuário, acesso a caminhos de rede bloqueados devido a restrições de acesso e a atribuição de senhas apropriadas para controle de acesso.

O quadro três define o controle de acesso a caminhos de rede e autenticação de usuários nos itens A.11.4.1 e A.11.4.2 respectivamente. O quadro quatro define a autenticação para o sistema operacional que é instalado em uma máquina e a senha que deve ser usada para controlar esse acesso nos itens A.11.5.2 e A.11.5.3 respectivamente.

Quadro 3 – Controle de acesso a rede e autenticação de usuários

A.11.4 Controle de acesso à rede		
<i>Objetivo:</i> Prevenir acesso não autorizado aos serviços de rede.		
A.11.4.1	Política de uso dos serviços de rede	<i>Controle</i> Os usuários devem receber acesso somente aos serviços que tenham sido especificamente autorizados a usar.
A.11.4.2	Autenticação para conexão externa do usuário	<i>Controle</i> Métodos apropriados de autenticação devem ser usados para controlar o acesso de usuários remotos.
A.11.4.3	Identificação de equipamento em redes	<i>Controle</i> Devem ser consideradas as identificações automáticas de equipamentos como um meio de autenticar conexões vindas de localizações e equipamentos específicos.
A.11.4.4	Proteção e configuração de portas de diagnóstico remotas	<i>Controle</i> Deve ser controlado o acesso físico e lógico para diagnosticar e configurar portas.

Quadro 4 – Controle de senhas

A.11.5 Controle de acesso ao sistema operacional		
<i>Objetivo:</i> Prevenir acesso não autorizado aos sistemas operacionais.		
A.11.5.1	Procedimentos seguros de entrada no sistema (<i>log-on</i>)	<i>Controle</i> O acesso aos sistemas operacionais deve ser controlado por um procedimento seguro de entrada no sistema (<i>log-on</i>).
A.11.5.2	Identificação e autenticação de usuário	<i>Controle</i> Todos os usuários devem ter um identificador único (ID de usuário), para uso pessoal e exclusivo, e uma técnica adequada de autenticação deve ser escolhida para validar a identidade alegada por um usuário.
A.11.5.3	Sistema de gerenciamento de senha	<i>Controle</i> Sistemas para gerenciamento de senhas devem ser interativos e assegurar senhas de qualidade.
A.11.5.4	Uso de utilitários de sistema	<i>Controle</i> O uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações deve ser restrito e estritamente controlado.

5 ISO 27001 APLICADA AO ACTIVE DIRECTORY E AO OPENLDAP EM AMBIENTE DE TESTE PARA FINS COMPARATIVOS EM PARAMETROS EQUIPARADOS.

5.1 Testes com o Microsoft Active Directory

Para iniciar um serviço de diretório usando o Active Directory Domain Services (ADDS) da Microsoft é preciso ter um IP estático para que sempre que o IP for consultado ele tenha um dono. Nesse experimento o IP do ADDS é 10.0.0.11 em um Windows Server 2012, o IP de outro servidor fazendo papel de Controlador de Domínio é 10.0.0.12 em um Windows Server 2008 R2 e o IP de uma estação de trabalho é 10.0.0.13 usando o Windows 8.

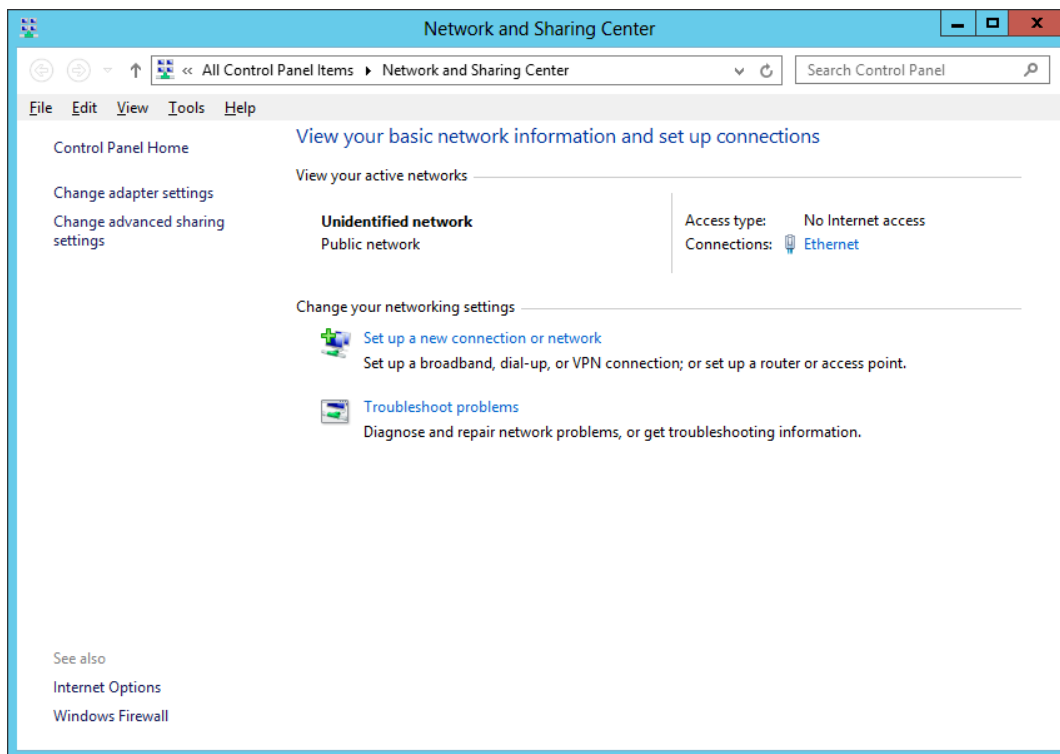
Também é preciso ter certeza de que o nome do servidor está correto porque após a instalação do serviço de diretório não será mais possível modifica-lo.

Ao fazer o primeiro acesso à um Windows server 2012 uma janela para gerenciamento do servidor é automaticamente aberta chamada de Server Manager. Pode-se verificar de imediato que todos os detalhes do servidor estão resumidos nessa janela.

5.1.1 Configurar IP Estático

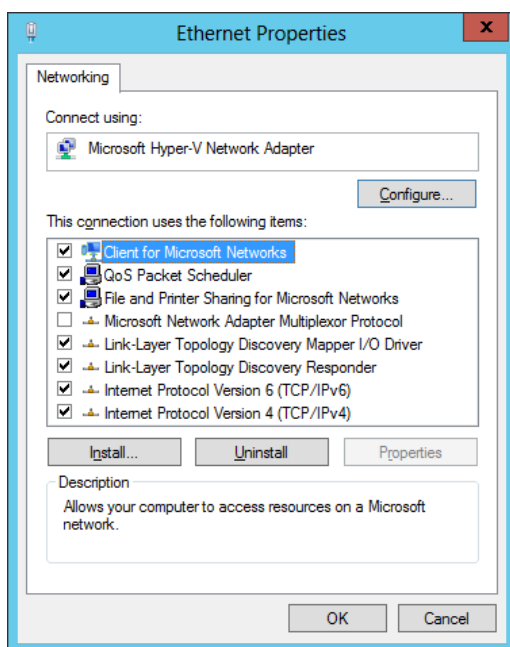
Para configurar o IP é preciso abrir o painel de controle e abrir o centro de compartilhamento e redes.

Figura 2 – Acesso ao Network and Sharing Center



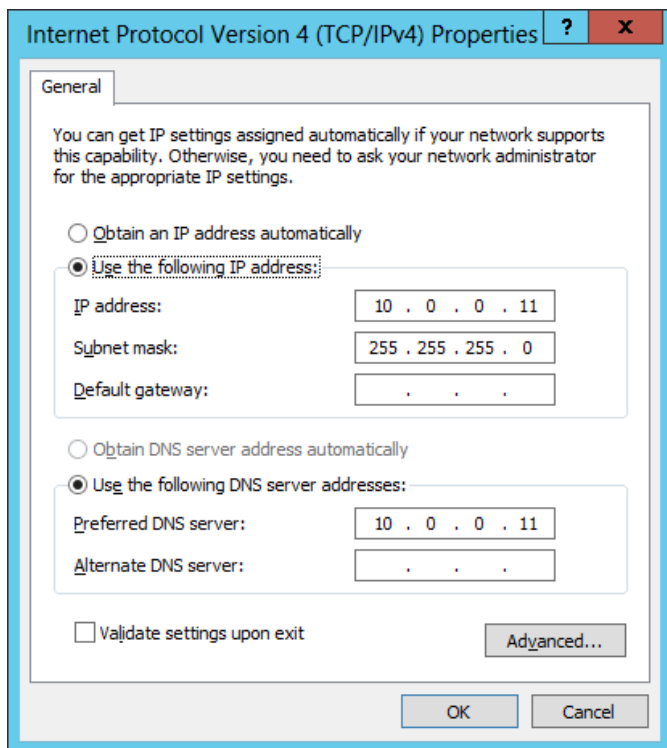
Após isso clicar em Ethernet, que é o nome dado por padrão a um adaptador de rede, e em seguida em propriedades:

Figura 3 – Propriedades do Adaptador de Rede



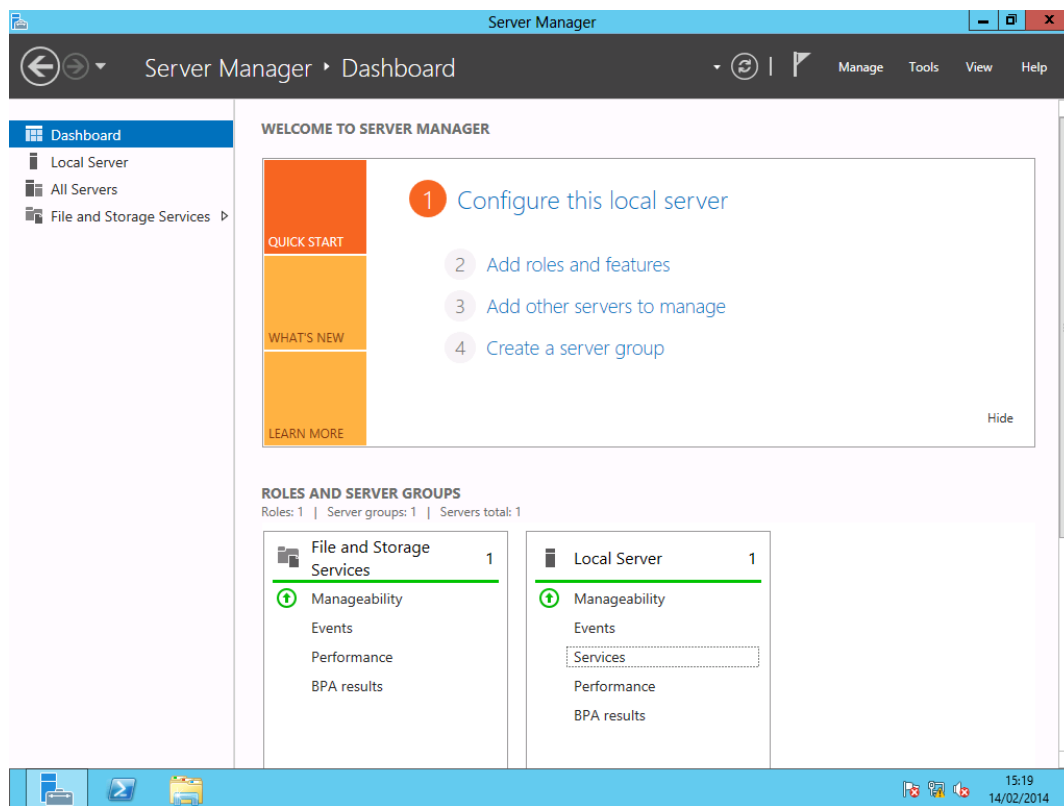
Para configurar o IP estático conforme já apresentado é preciso selecionar o protocolo de internet versão 4 (TCP/IPv4) e clicar em propriedades:

Figura 4 – Propriedades do IPv4 no Adaptador Ethernet.



Ao iniciar o servidor com Server 2012 é observado uma interface gráfica praticamente auto explicativa. Conforme imagem abaixo:

Figura 5 – Gerenciador do Servidor no Windows Server 2012 R2

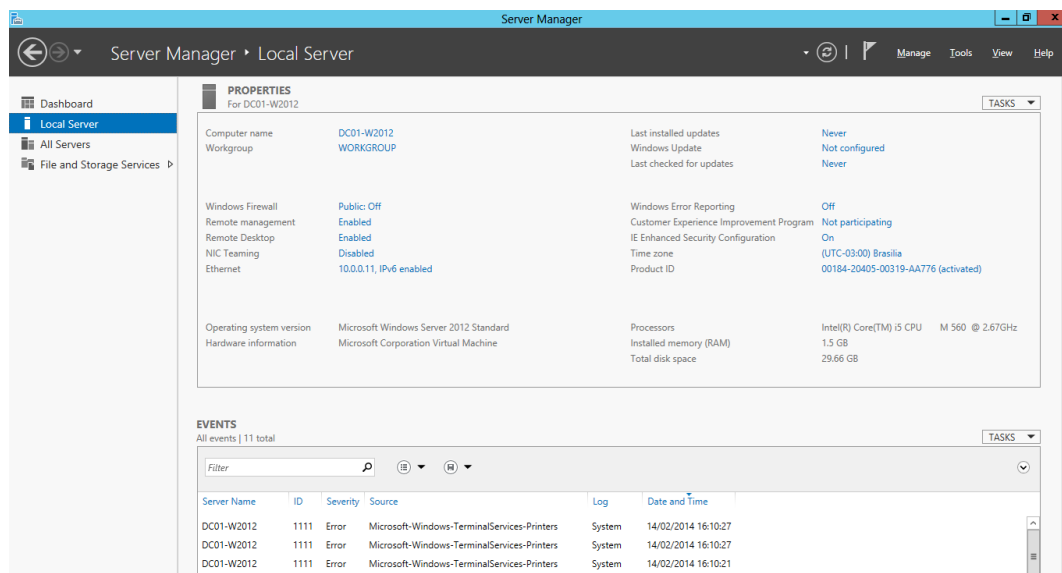


Dashboard é a tela em que são apresentados os serviços ou roles em caráter de resumo, apresentando se a alguma anormalidade.

5.1.2 Verificação do Nome do Servidor

Para verificação do nome do servidor é preciso clicar em Local Server. O Local Server é onde podem ser encontrado todos os detalhes sobre o servidor que está sendo configurado.

Figura 6 – Detalhes do Servidor no Gerenciador do Servidor



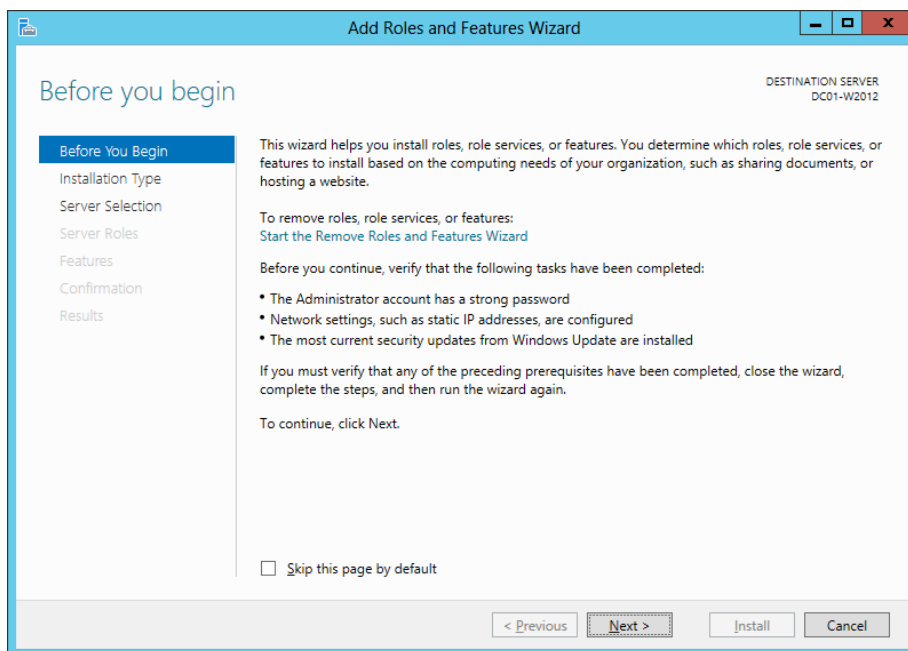
Uma vez na tela do Local Server, observa-se que a primeira propriedade do computador é o nome do mesmo. Para alterá-lo basta clicar no nome e alterá-lo colocando a credencial administrativa do servidor. Essa credencial é criada para acesso ao servidor no momento da instalação do sistema operacional.

Nesse experimento o nome do servidor é DC01-W2012.

5.1.3 Instalação do Serviço de Diretório

Para ativar o serviço de diretório do Windows server 2012 é preciso ativar a função ADDS, ao clicar em Add roles and features (Adicionar funções e características) na tela Dashboard é aberto um Wizard, assistente de instalação, para facilitar o acesso as opções de configuração do servidor, conforme figura abaixo:

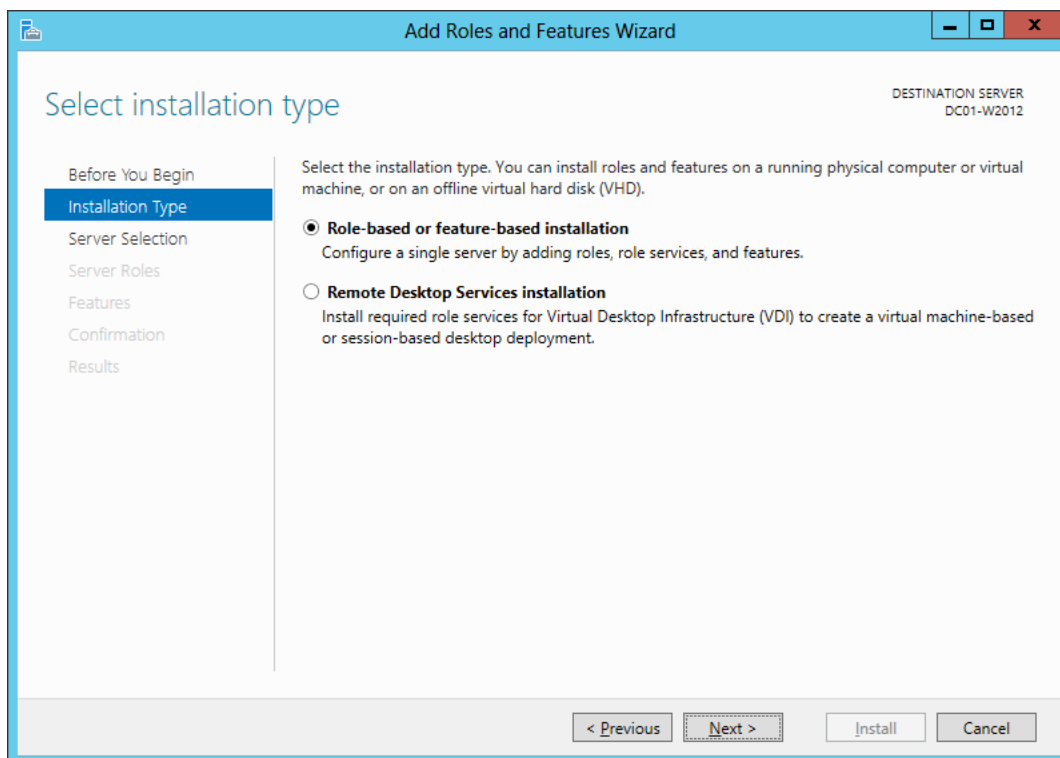
Figura 7 – Assistente para Adicionar Funcionalidades ao Servidor



Nesse *Wizard* o Windows faz sugestões baseadas nas configurações já realizadas para melhorar o desempenho das funções escolhidas e sugere algumas features (características) que são necessárias para que as funções escolhidos correspondam as expectativas do administrador.

Logo em seguida o Windows oferece duas opções de instalação para as novas funções, uma em que funções serão instaladas no servidor local e outra para criar uma função em outro servidor virtual via rede conforme figura a baixo:

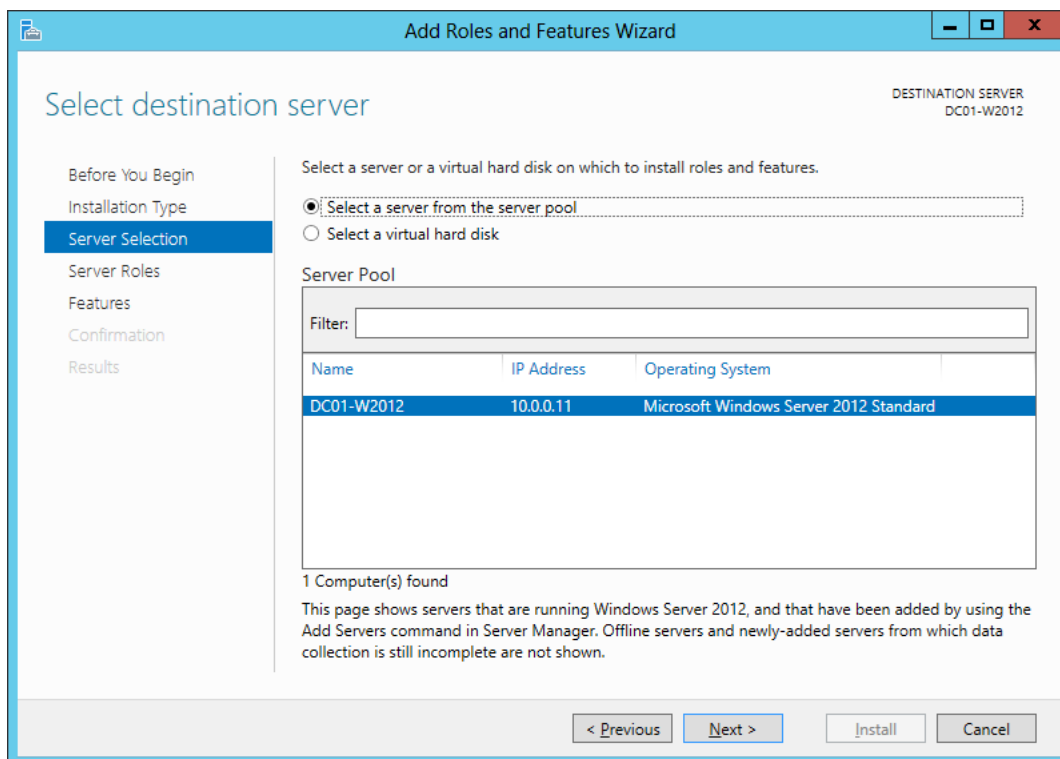
Figura 8 – Tela do Assistente para Escolha do Tipo de Instalação



Nesse experimento será feita a instalação no servidor local.

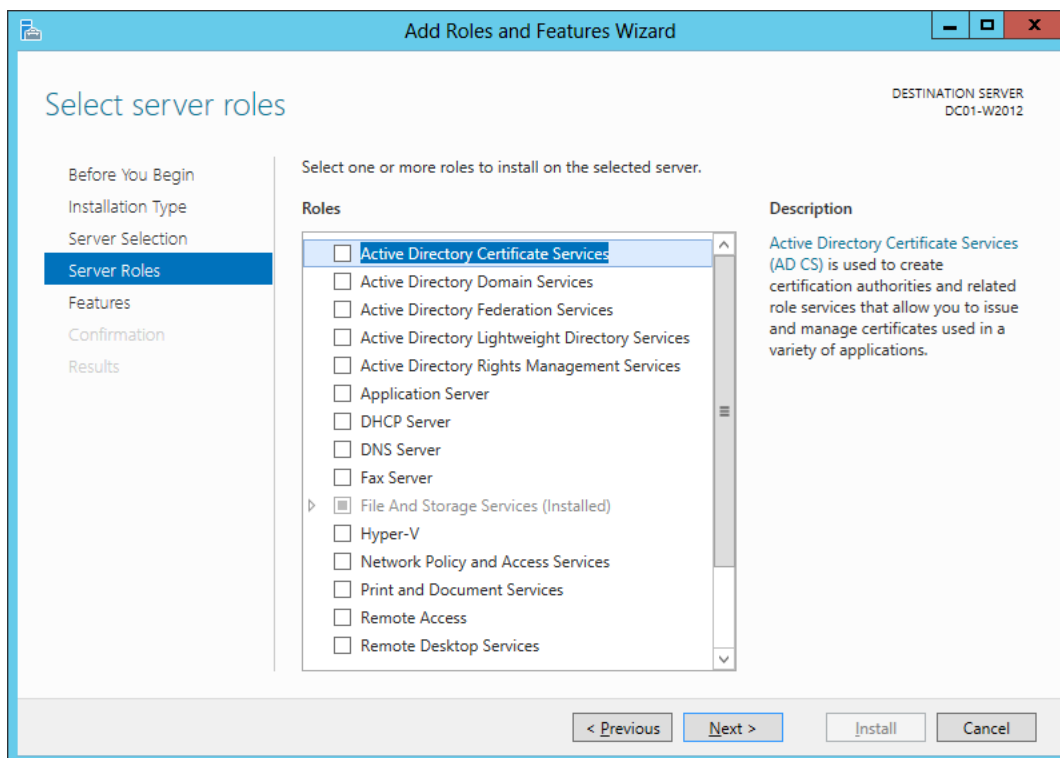
O Windows em seguida pergunta se existe um pool de servidores onde é possível escolher um servidor na rede que não seja o local para fazer a instalação do serviço. Porém nesse experimento esse servidor é o primeiro da rede e só ele poderá ser escolhido.

Figura 9 – Tela do Assistente para Escolha do Disco Virtual para Instalação de Funções



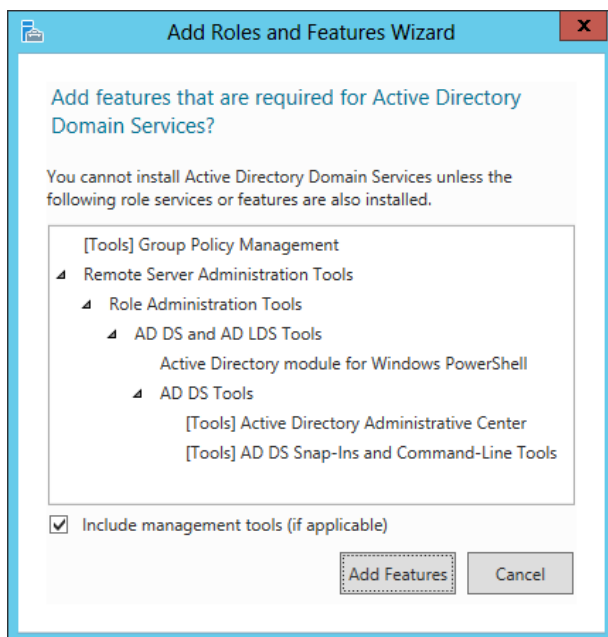
Como próximo passo, é aberta no wizard a tela para escolha dos serviços a serem instalados. Nessa tela além de terem vários serviços como opção para instalação ainda existe uma breve descrição sobre o que cada serviço pode proporcionar, conforme abaixo:

Figura 10 – Tela do Assistente para Escolha das Funções do Servidor



Ao clicar em Active Directory Domain Services (ADDS), é aberta uma janela de sugestões para instalações de características (features), que vão permitir o funcionamento por completo da função escolhida. Se essas features não forem instaladas o Windows impedirá a instalação do serviço.

Figura 11 – Tela do Assistente de Resumo de Funções Escolhidas



Ao clicar em Add Features, o administrador aceita a instalação dos pré-requisitos.

O Windows server também possibilita a instalação de outros serviços simultaneamente. A Microsoft faz a recomendação de sempre instalar no servidor que terá o ADDS o serviço DNS. O DNS é o serviço que dá nome aos computadores e servidores participantes do domínio. Ao invés de procurar um computador pelo IP para armazenar documentos pode-se ter o catálogo de nome dos computadores para facilitar os acessos.

Nesse experimento o DNS se faz necessário devido a necessidade de toda organização ter um serviço DNS e a motivação deste trabalho é de simular a realidade empresarial.

Para instalar o DNS basta clicar também no serviço DNS que apresentado no wizard para seleção de funções. Da mesma forma que quando o serviço de ADDS é selecionado o wizard apresenta as features necessárias para o correto funcionamento do serviço.

Figura 12 - Tela do Assistente Questionando a Instalação do Serviço DNS

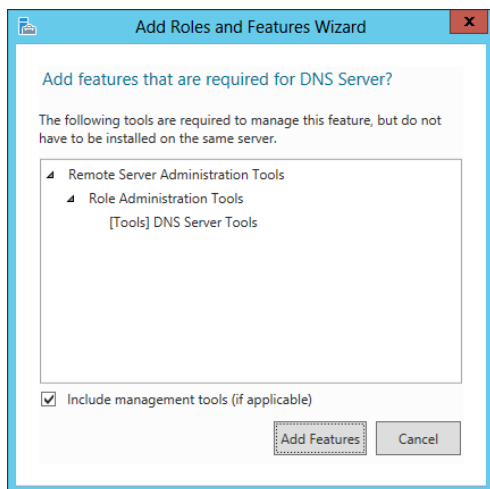
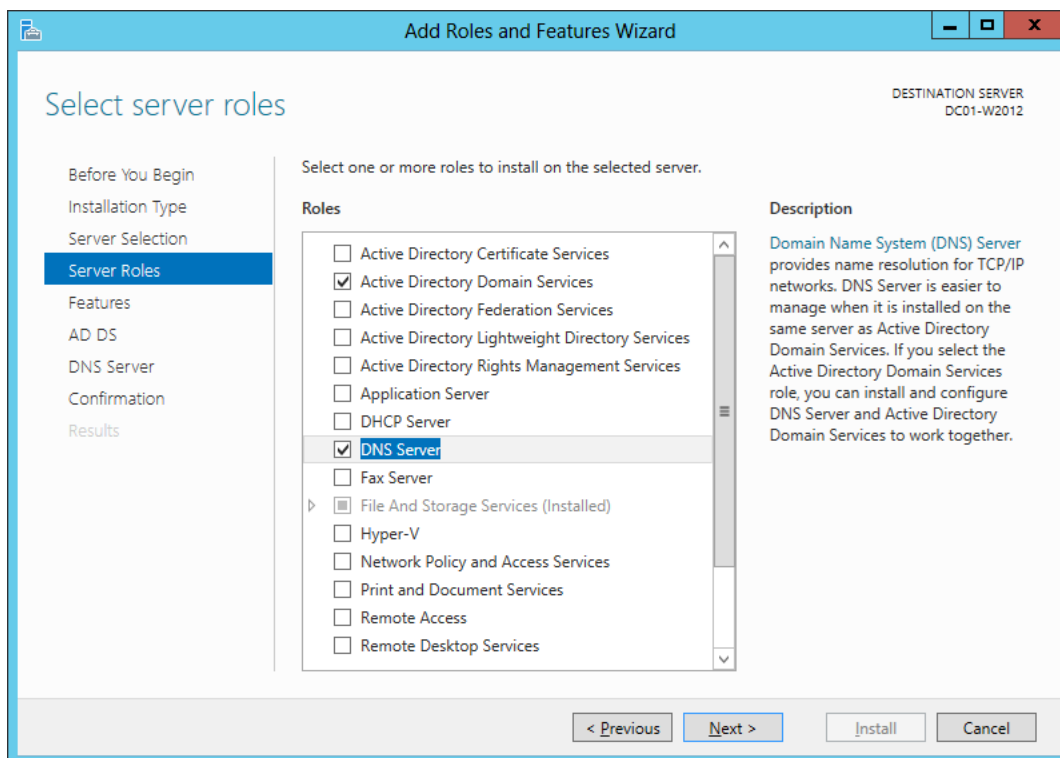
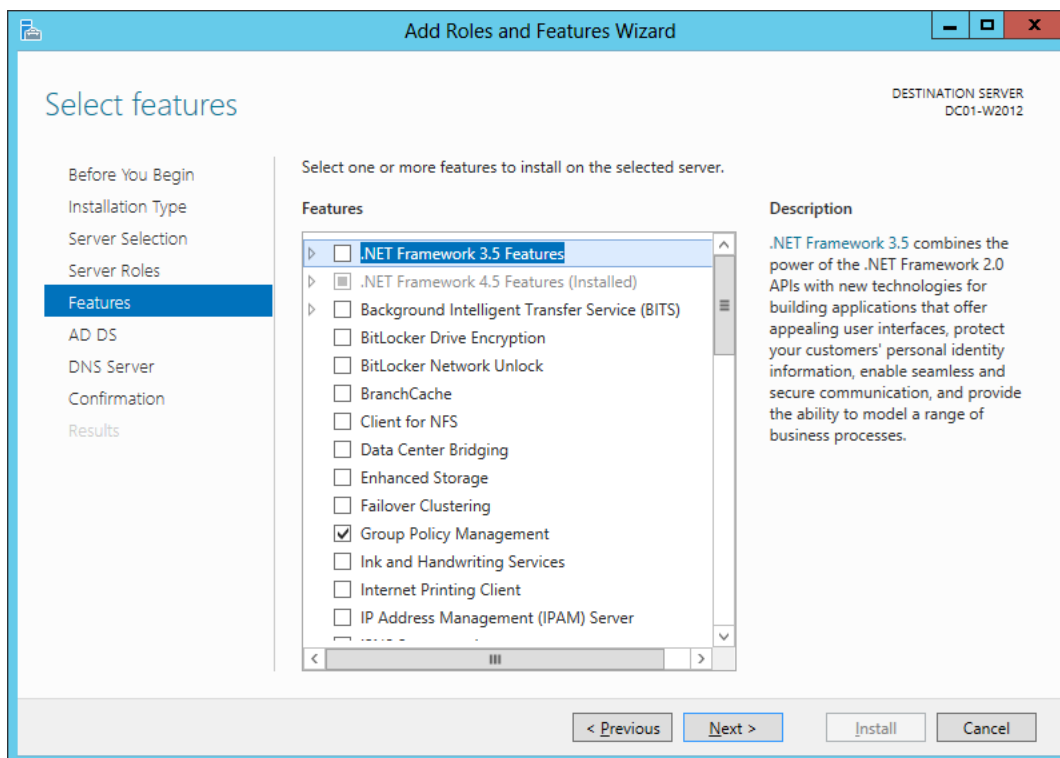


Figura 13 - Tela do Assistente Adicionando a Função de DNS



Agora que os dois serviços principais estão selecionados basta clicar em next. Em seguida o wizard leva o administrador para a seleção de features, onde é visível que algumas delas já estão marcadas para serem instaladas, essas são as que o wizard sugeriu como pré-requisito para o correto funcionamento dos serviços escolhidos.

Figura 14 – Tela do Assistente Adicionando o Group Policy Manager



Ao clicar em next, o wizard mostra algumas recomendações da Microsoft para o melhor funcionamento do sistema, e ainda faz a descrição de algumas features que são instaladas junto com o ADDS.

Figura 15 – Tela do Assistente Alertando Sobre o Serviço ADDS

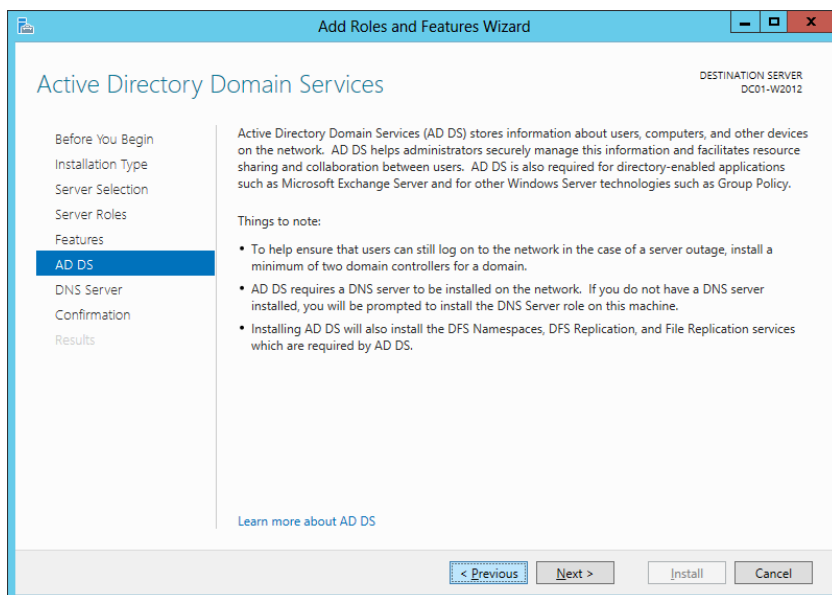
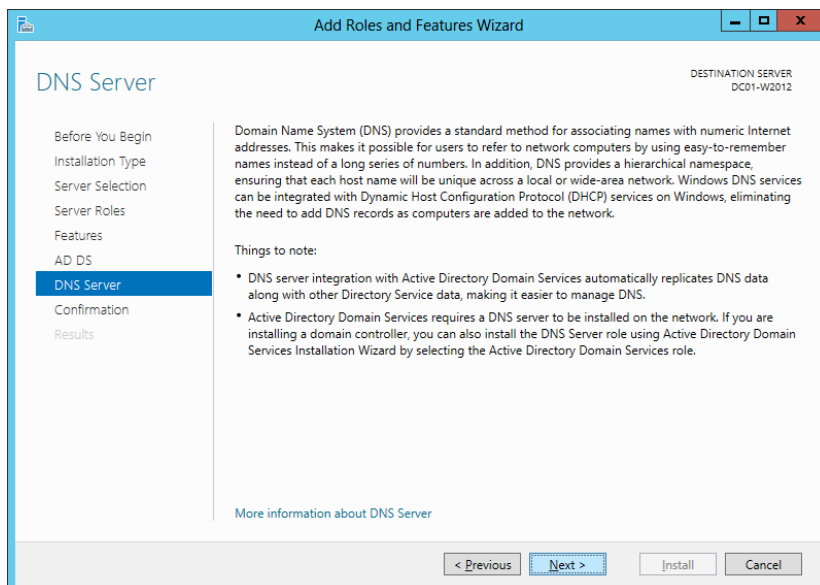
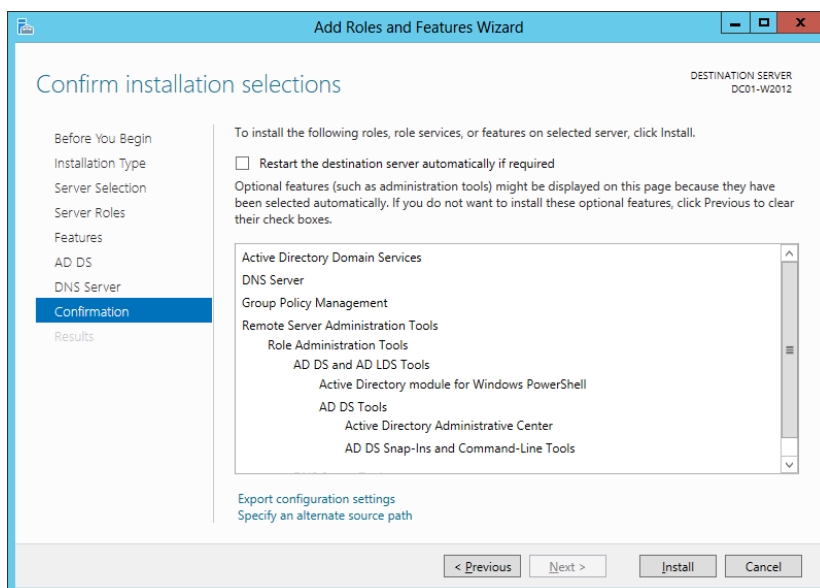


Figura 16 – Tela do Assistente Alertando Sobre o Serviço DNS



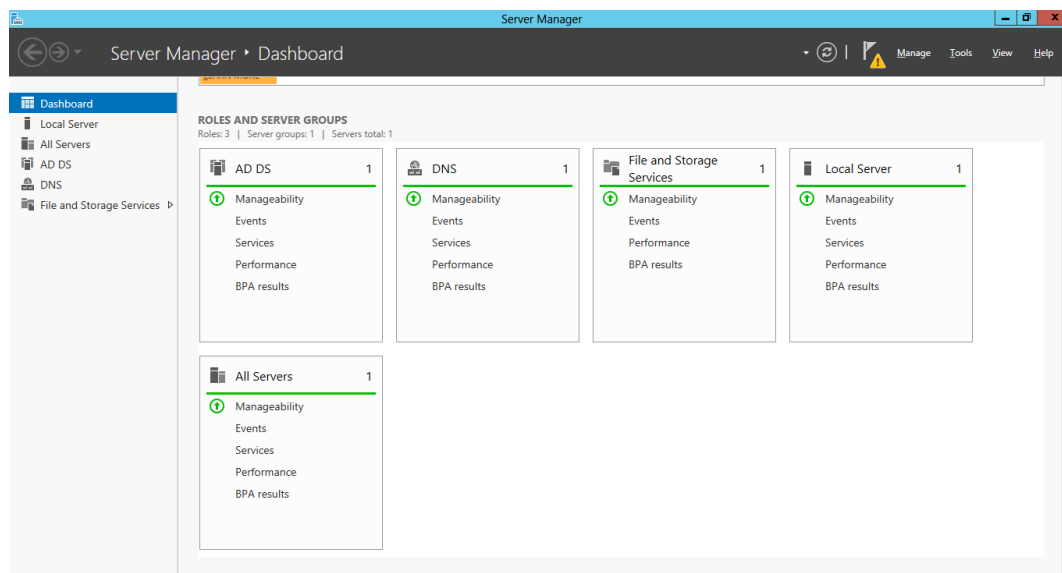
Continuando adiante o wizard mostra por fim o resumo de todos os serviços e features que serão instalados enquanto questiona se deve instalar os mesmos, conforme figura abaixo:

Figura 17 – Tela do Assistente Resumindo Todas as Funções



Depois da Instalação outros serviços são mostrados na tela de resumo de serviços do Dashboard, são eles o ADDS, o DNS, Todos os Servidores, Serviço de armazenamento e Servidor Local conforme figura abaixo:

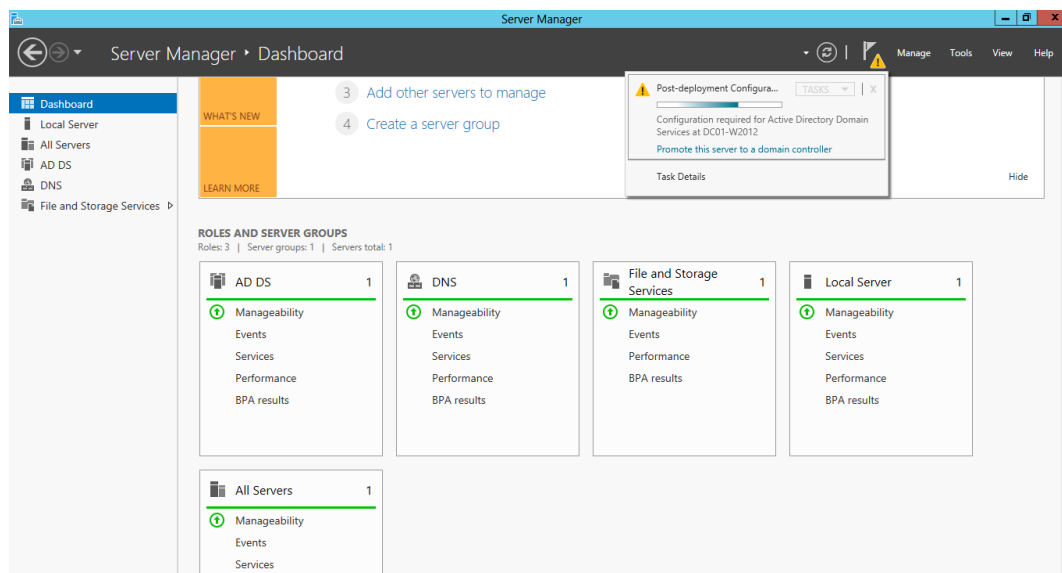
Figura 18 – Tela da Gerencia do Servidor com Serviços Instalados



Em um segundo momento, em seguida da instalação dos serviços do ADDS e DNS, um sinal de exclamação fica visível na parte superior da janela server manager. Esse sinal de exclamação significa que o servidor precisa avisar algo para o administrador e neste caso específico avisa ao administrador que deve ser feita continuação da instalação dos serviços recém instalados.

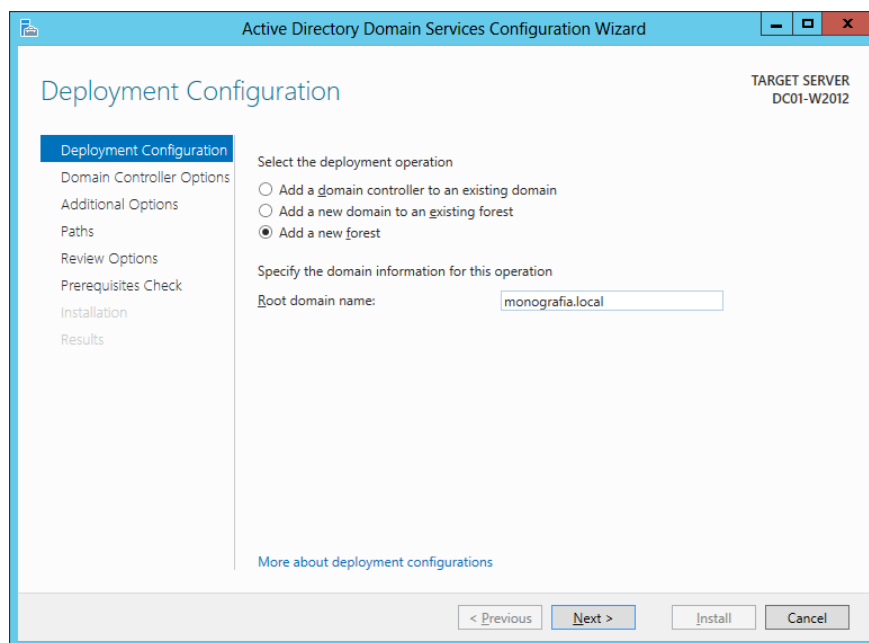
A primeira ação que deve ser tomada após a instalação do ADDS é promover o servidor e torna-lo um Controlador de Domínio, basta acessar o link Promote this server to a domain controller, conforme figura abaixo.

Figura 19 – Gerenciador do Servidor Apresentando a Opção de Controlador de Domínio



Logo após acessar o link do domain controller (DC), outro wizard é iniciado para auxiliar na configuração do novo controlador de domínio.

Figura 20 – Assistente para Configuração do ADDS

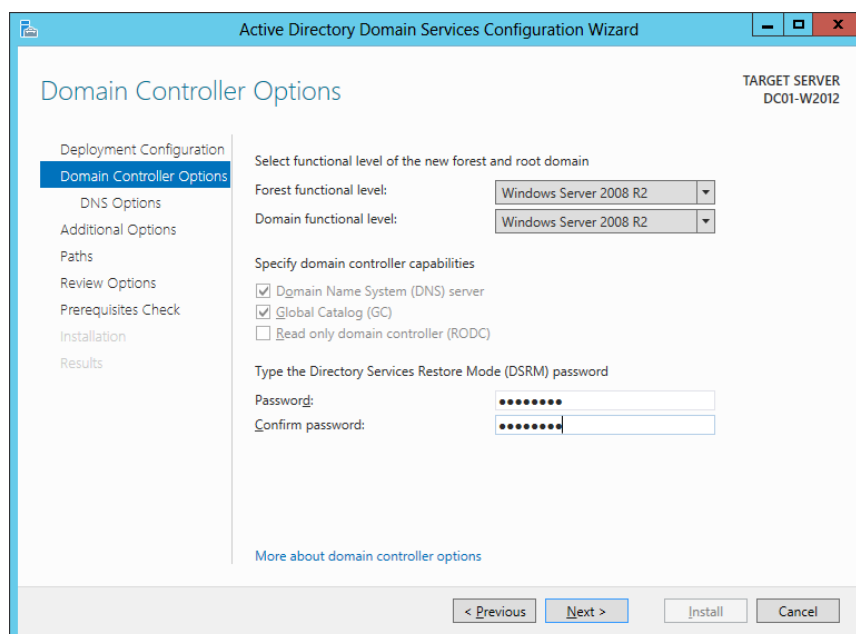


Conforme pode ser observado na figura acima, o wizard traz uma série de etapas que devem ser cumpridas para que o novo serviço fique com funcionamento correto. A primeira etapa é escolher a operação de instalação e como esse é o primeiro DC deve-se adicionar uma nova floresta. Um conjunto de domínios é uma

floresta, dessa forma para começar uma floresta é preciso então configurar o primeiro domínio que terá o nome de MONOGRAFIA.LOCAL.

Após iniciar uma nova floresta é preciso definir o nível funcional. O nível funcional determina o nível de funções que farão parte do domínio e de todos os servidores do domínio. Se no domínio houver um servidor com Windows Inferior ao 2012 então o 2012 se comunicará com esse servidor no nível de sua capacidade. No caso desse experimento um outro controlador de domínio será inserido no domínio e seu Windows é o Server 2008 R2, portanto, o nível funcional desse domínio será Windows Server 2008 R2.

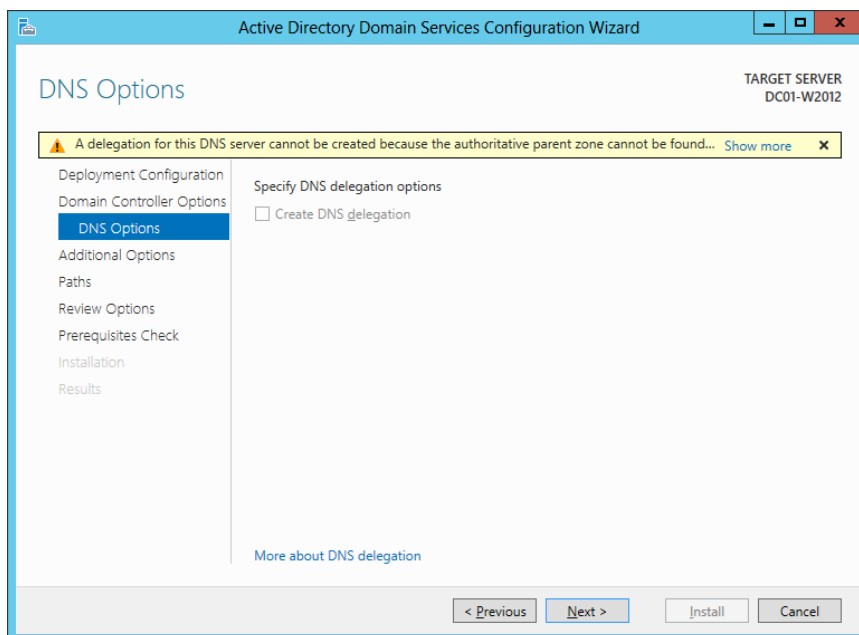
Figura 21 – Assistente para Configuração de Nível Funcional do ADDS



Ainda nesta etapa é preciso definir uma senha para que em caso de ser necessário restaurar serviços ser possível resgata-los.

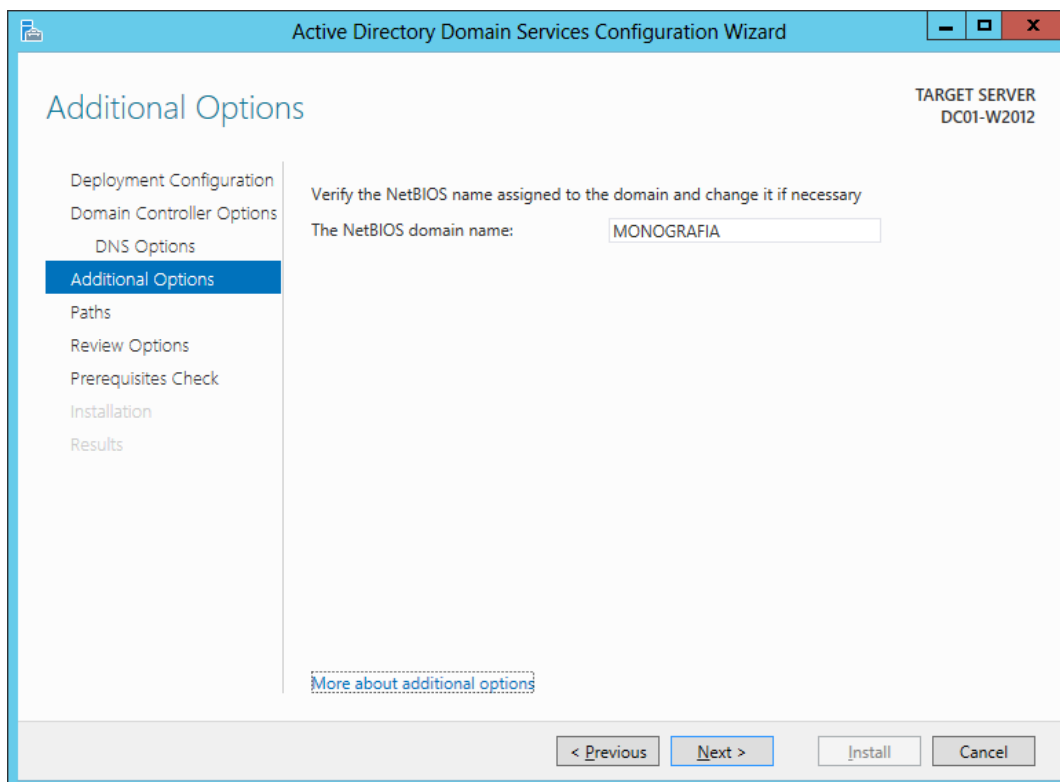
No próxima etapa não é possível delegar nenhuma opção do serviço a nenhum outro servidor no momento devido a este servidor ser o primeiro do domínio.

Figura 22 – Erro Relacionado ao DNS na Configuração do ADDS



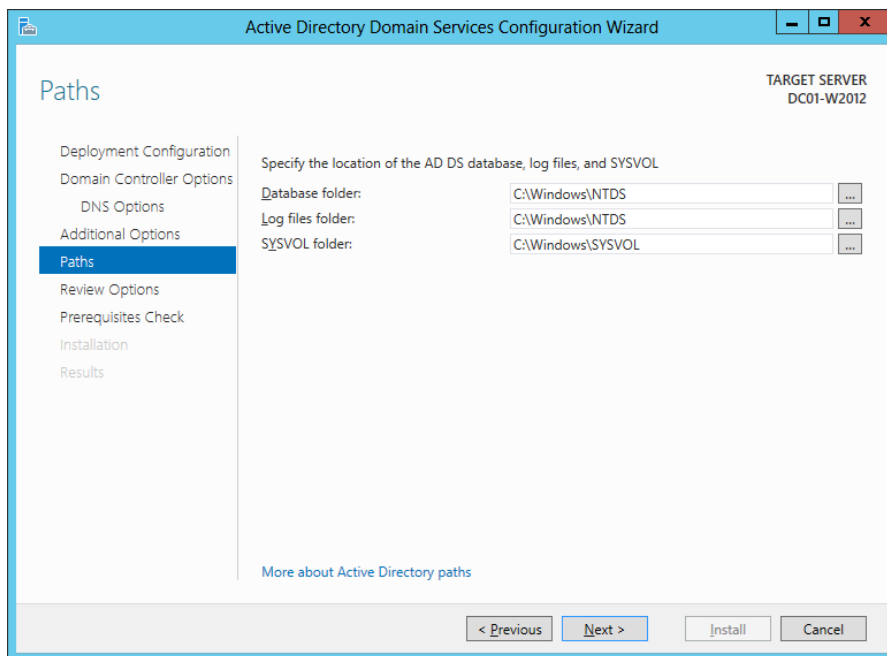
Na etapa subsequente o nome Netbios já vem preenchido com o nome principal do domínio, neste caso é preciso aceitar a opção e continuar com a configuração.

Figura 23 – Assistente para Configuração do Nome NetBIOS do ADDS



No próximo passo, o wizard questiona quanto o local do armazenamento do banco de dados com a pasta NTDS e o local para armazenamento dos scripts e políticas com a pasta SYSVOL, no caso do experimento essas pastas serão armazenadas no próprio servidor.

Figura 24 – Assistente para Localização da Base de Dados do ADDS



Em Seguida o wizard apresenta um resumo das configurações que serão instalados e em seguida verifica se os arquivos pré-requisitos estão instalados e tem o início da instalação.

Figura 25 – Resumo da Configuração do ADDS

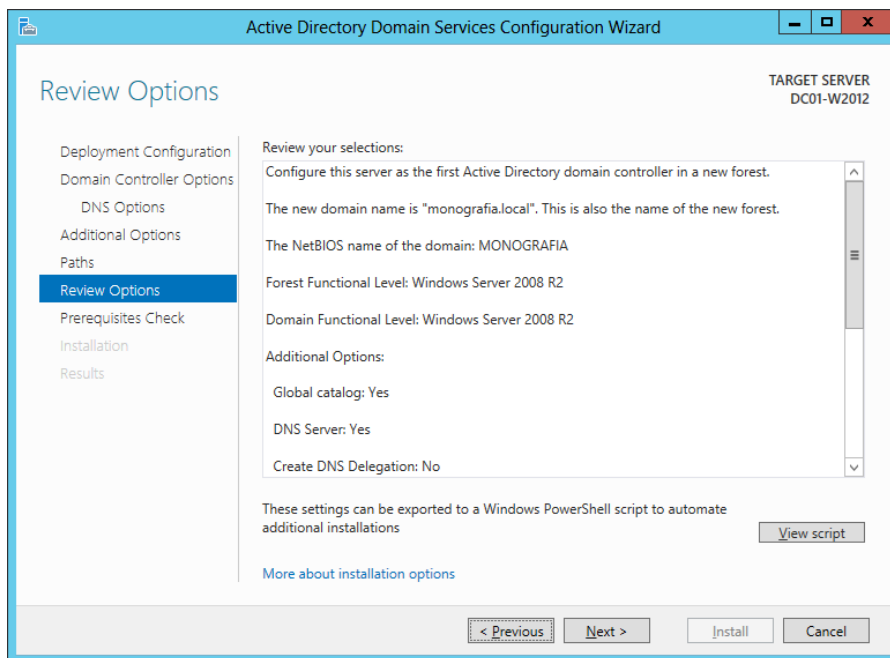
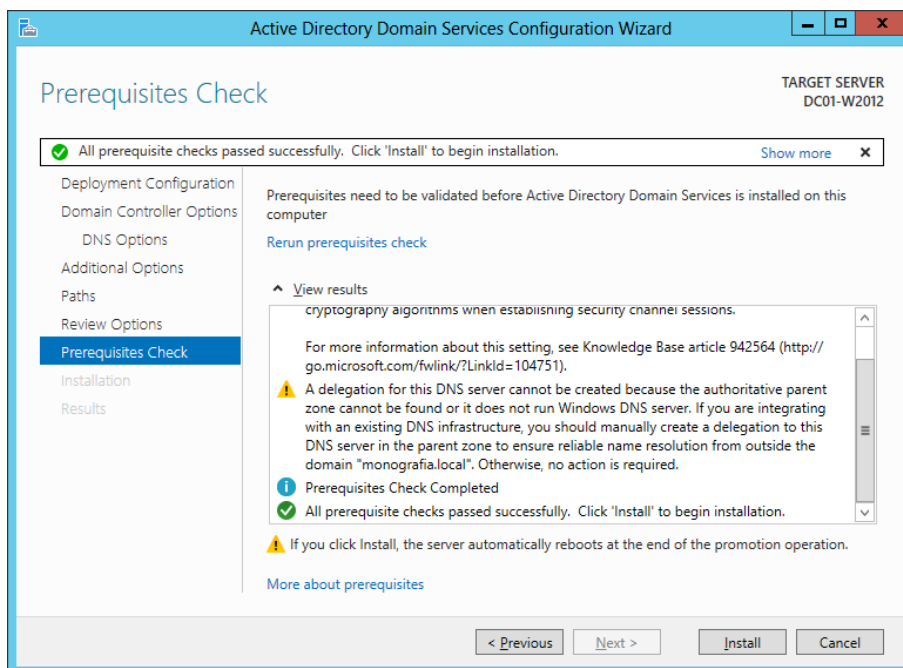


Figura 26 – Checagem de Pré-requisitos do ADDS



5.1.4 Desafio ao Active Directory

Uma vez criado o domínio, inicia-se a fase de aplicação do planejamento da infraestrutura do domínio.

Esse experimento tem o foco de acompanhar algumas exigências comuns das políticas de segurança mais utilizadas pela maioria das empresas de grande porte, incluindo governo federal e simula-las em laboratório conforme o capítulo quatro lista nas tabelas da ISO 27001

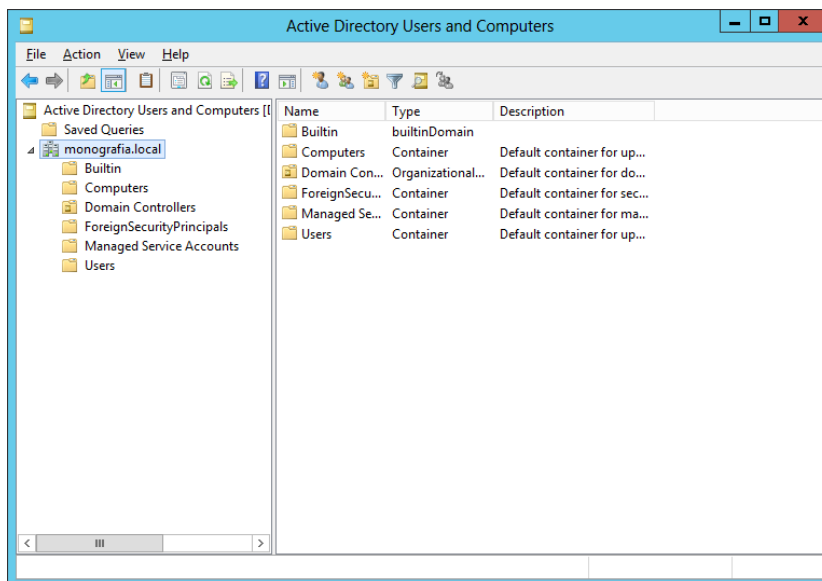
Entre as exigências de segurança mais conhecida pela tecnologia da informação estão, a autenticação de usuários, ou seja, cada funcionário de uma empresa deve ter um usuário cadastrado para fazer acesso aos recursos de tecnologia da empresa, o acesso restrito a pastas e documentos, somente pessoas autorizadas podem ter acesso a pastas específicas, e senhas para acesso do usuário ao domínio com nível de dificuldade específico para cada grupo de usuários que impeçam acesso não autorizado de funcionários aos equipamentos da empresa.

Para que seja possível simular esse ambiente é preciso cadastrar novos usuários, cadastrar novos grupos de usuários, incluir computadores no domínio, criar pastas para cada departamento no servidor de arquivos e aplicar políticas de gerenciamento para controle de acesso às pastas por grupos de usuários.

5.1.5 Criação de Usuários

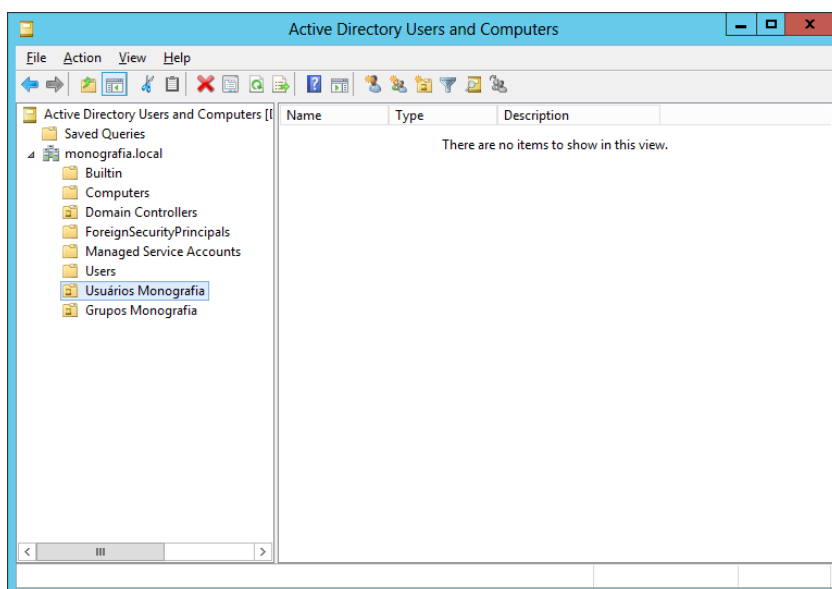
Para adicionar usuários no domínio é preciso acessar as ferramentas no link tools da tela do server manager. A primeira ferramenta usada é a usuários e computadores do Active Directory (Active Directory Users and Computers).

Figura 27 – Usuários e Computadores do Active Directory



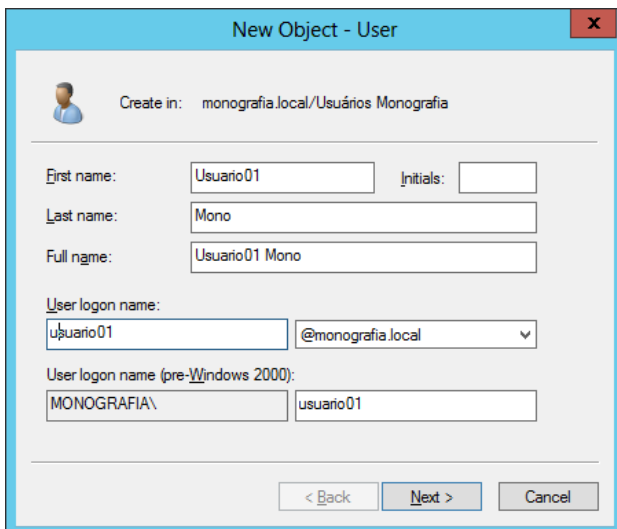
Ao selecionar o novo domínio são abertas as pastas para gerenciamento de computadores e usuários do domínio. Para esse experimento serão criados duas novas pastas do domínio, também chamadas de Unidades Organizacionais (OU), uma para usuários e outra para grupos de usuários. A pasta Users traz usuários padrão do domínio como o usuário administrador usado para acessar o servidor do ADDS.

Figura 28 – Criação das Unidades Organizacionais



O padrão de usuários é usuárioXX e senha 123456 conforme figuras abaixo:

Figura 29 – Assistente para Criação de Novo Usuário

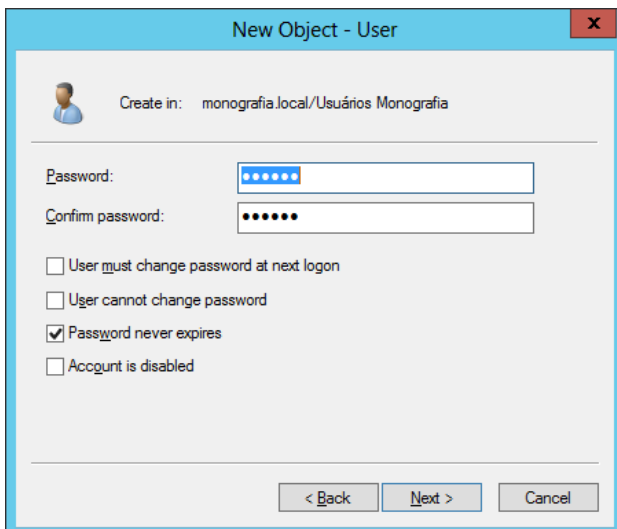


The dialog box is titled "New Object - User" and has a close button (X) in the top right corner. It contains a user icon and the text "Create in: monografia.local/Usuários Monografia". The form fields are as follows:

First name:	Usuario01	Initials:	
Last name:	Mono		
Full name:	Usuario01 Mono		
User logon name:	usuario01		@monografia.local
User logon name (pre-Windows 2000):	MONOGRAFIA\ usuario01		

At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

Figura 30 – Assistente para Criação de Senha para Novo Usuário



The dialog box is titled "New Object - User" and has a close button (X) in the top right corner. It contains a user icon and the text "Create in: monografia.local/Usuários Monografia". The form fields are as follows:

Password:
Confirm password:

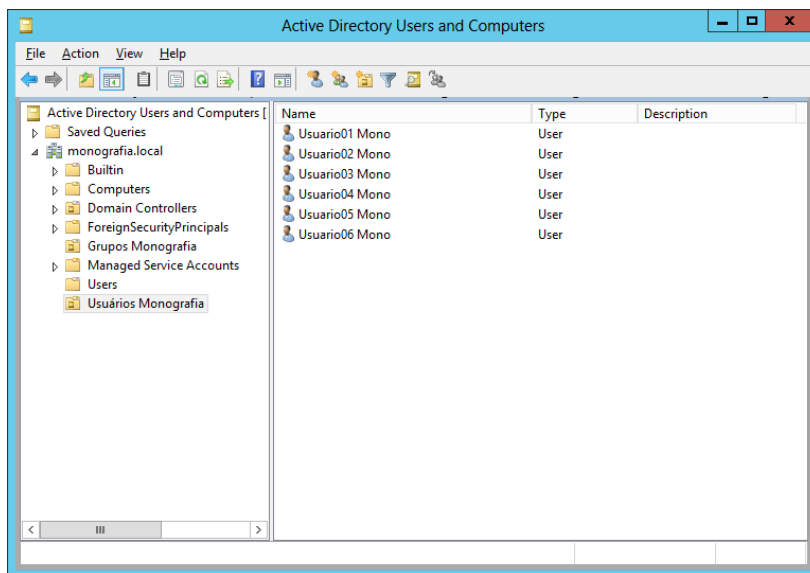
Below the password fields, there are four checkboxes:

- ☐ User must change password at next logon
- ☐ User cannot change password
- ☒ Password never expires
- ☐ Account is disabled

At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

Foram criados 6 usuários para este experimento.

Figura 31 – Novos Usuários Criados na OU



5.1.6 Criação dos Grupos

Para criar os grupos basta clicar na nova OU grupos e cria-los, porém, é importante separar o tipo do grupo a ser criado neste experimento será usado somente o grupo local, devido a ser apenas um DC.

Figura 32 – Container de Grupos do Domínio

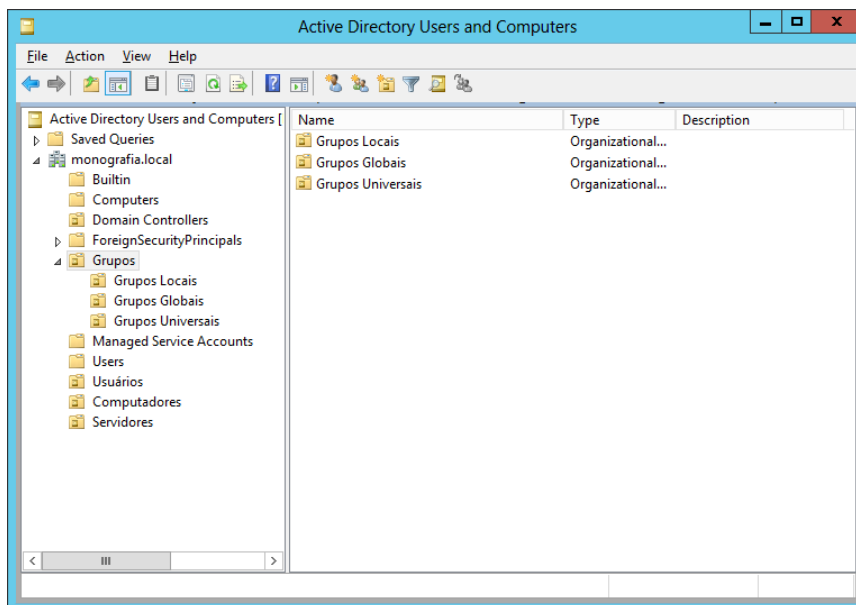


Figura 33 – Assistente para Criação de Novo Grupo

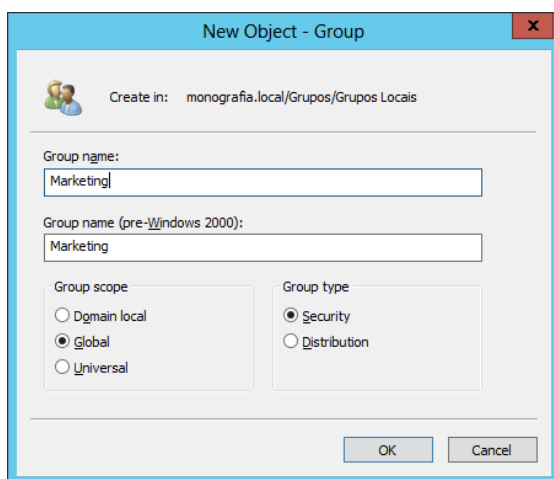
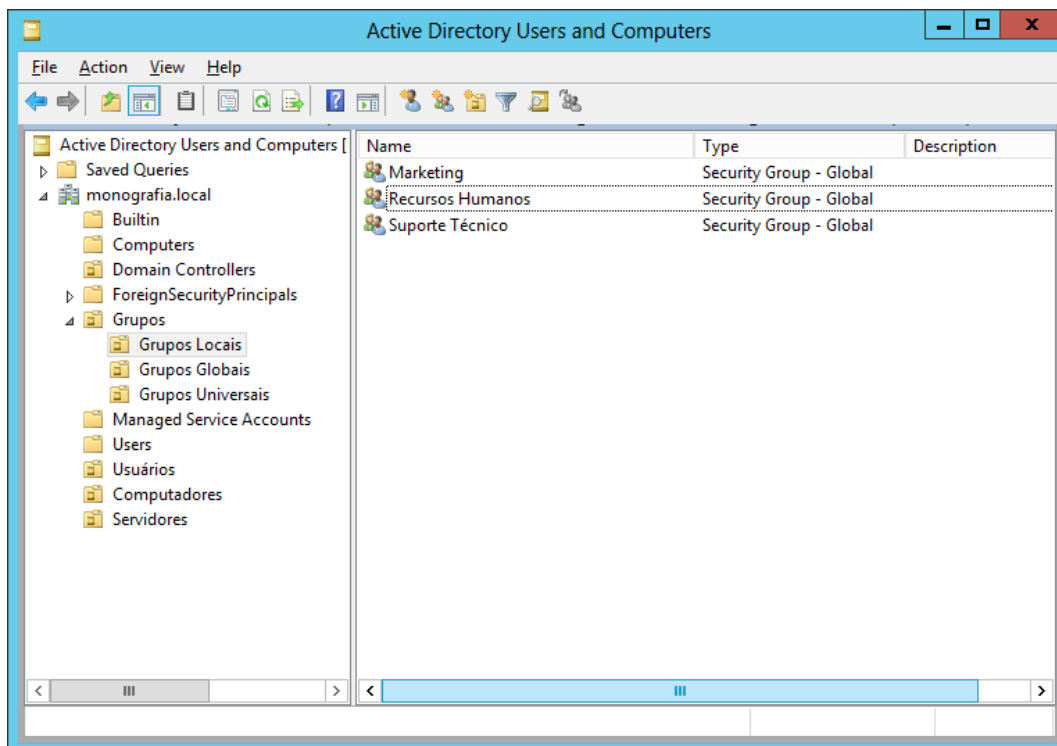


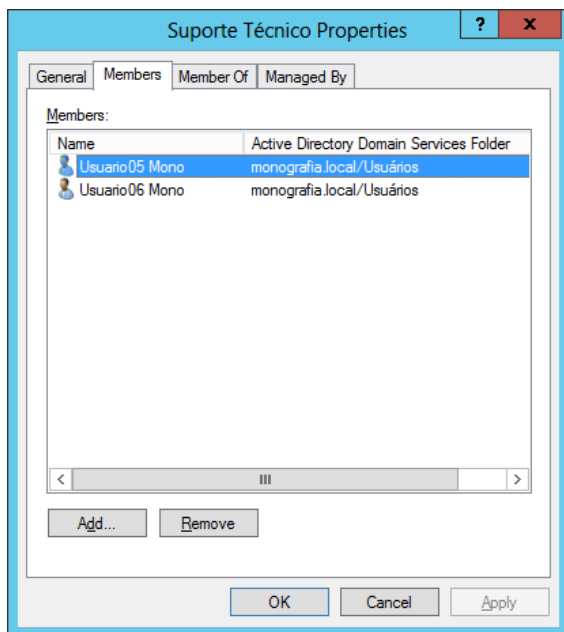
Figura 34 – Grupos Novos Criados no Container de Grupos



Foram criados os grupos de Marketing, Recursos Humanos e Suporte Técnico. De acordo com a uma política de segurança comum, cada departamento da empresa acessa somente os arquivos e pastas respectivos e tem acesso restrito ao dos outros departamentos. No caso deste experimento o grupo Marketing irá acessar somente a pasta Marketing, o grupo Recursos Humanos irá acessar somente a pasta Recursos Humanos e o grupo suporte acessará todas as pastas incluindo a pasta Suporte Técnico.

Os usuários 01 e 02 serão do departamento de Marketing, os usuários 03 e 04 serão do departamento de Recursos Humanos e os usuários 05 e 06 serão do suporte técnico.

Figura 35 – Propriedades do Grupo Suporte Técnico

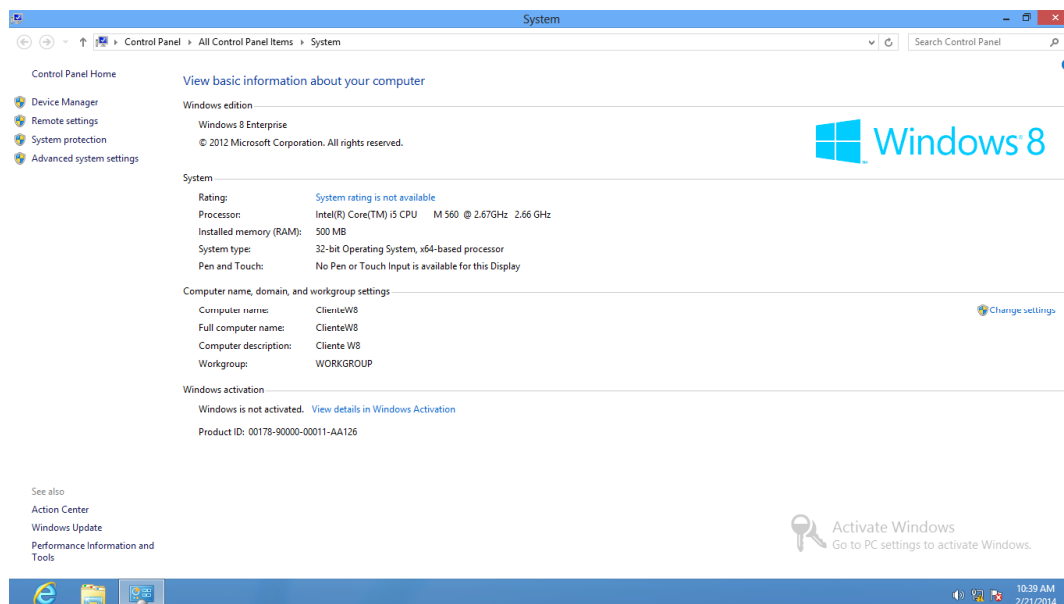


5.1.7 Inclusão de Servidores e Clientes no Domínio

Para incluir os servidores e estações de trabalho no domínio é preciso entrar nas propriedades dos computadores e modificar o nome. Para este experimento utilizando o ADDS será usado um servidor de arquivo Windows Server 2008 R2 e uma estação de trabalho Windows 8.

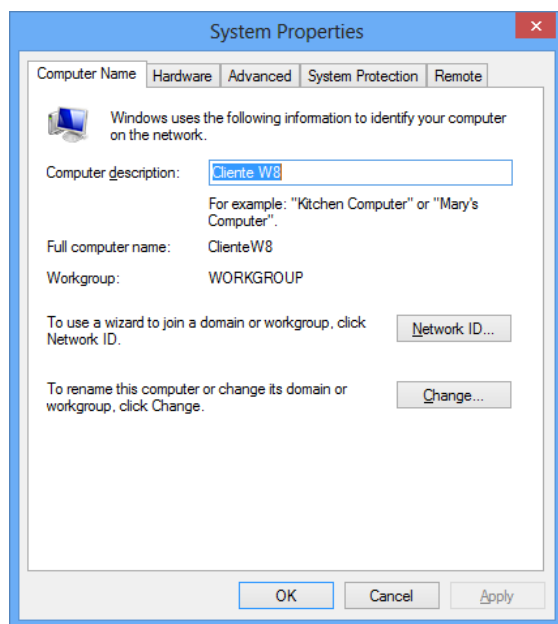
Para incluir a estação de trabalho no domínio é preciso modificar as configuração da estação acessando o link Change Settings.

Figura 36 – Tela de Detalhes do Sistema da Máquina Cliente



Neste caso será preciso acessar o link *Change* do janela de propriedades do computador.

Figura 37 – Propriedades do Sistema



Para este experimento a estação de trabalho terá o nome de cliente01 e fará parte do domínio monografia.local.

Figura 38 – Modificando o Nome e o Domínio

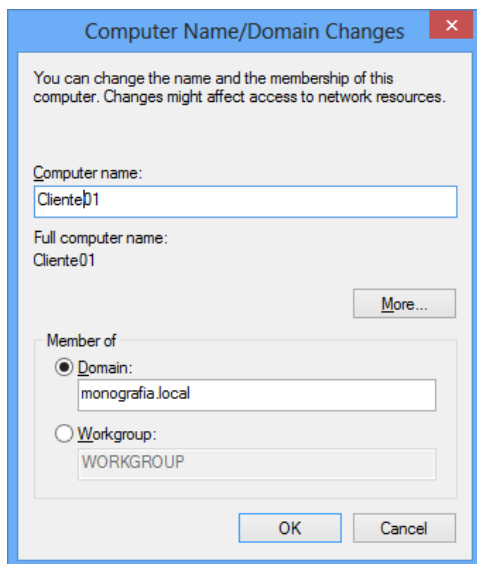


Figura 39 – Confirmação de Alteração de Domínio para Monografia.local

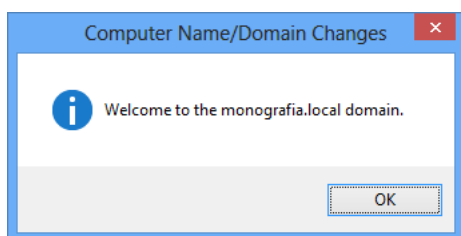
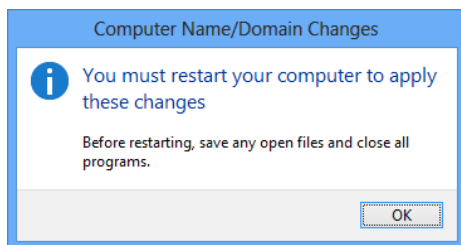


Figura 40 – Requisição para Reiniciar o Computador



Agora que a estação de trabalho está no domínio é preciso fazer o acesso com algum usuário criado no ADDS para fazer a verificação do ingresso no domínio. Para este caso o acesso pode ser feito com o usuario01 porém, para que o usuário possa fazer acesso remoto a máquina virtual é preciso adicionar o usuário no grupo padrão do ADDS de acesso remoto WinRMRemoteWMIUsers_.

Figura 41 – Grupo para Acesso Remoto

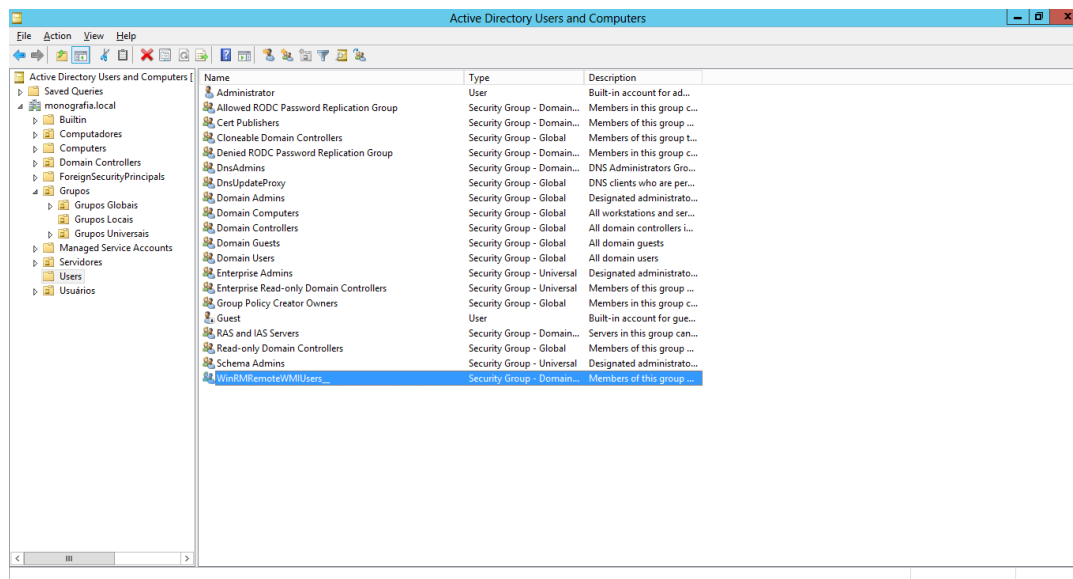
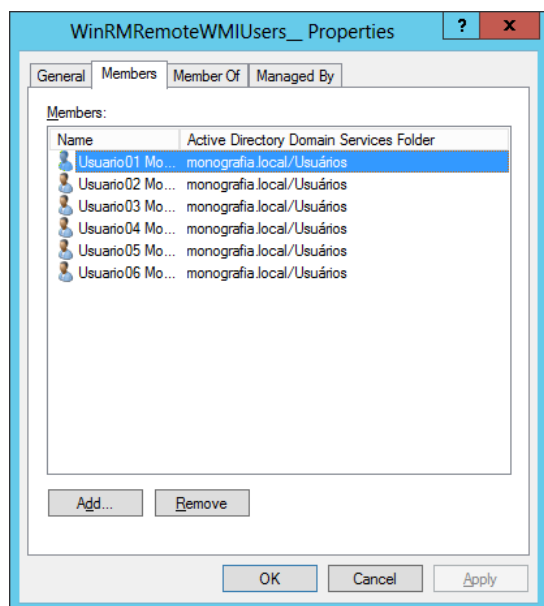


Figura 42 – Membros Pertencentes ao Grupo de Acesso Remoto



No cliente acessar com o usuário do domínio.

Figura 42 – Autenticação do Usuário no Domínio

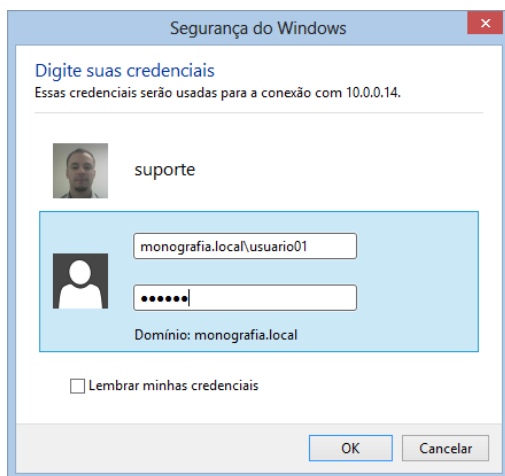
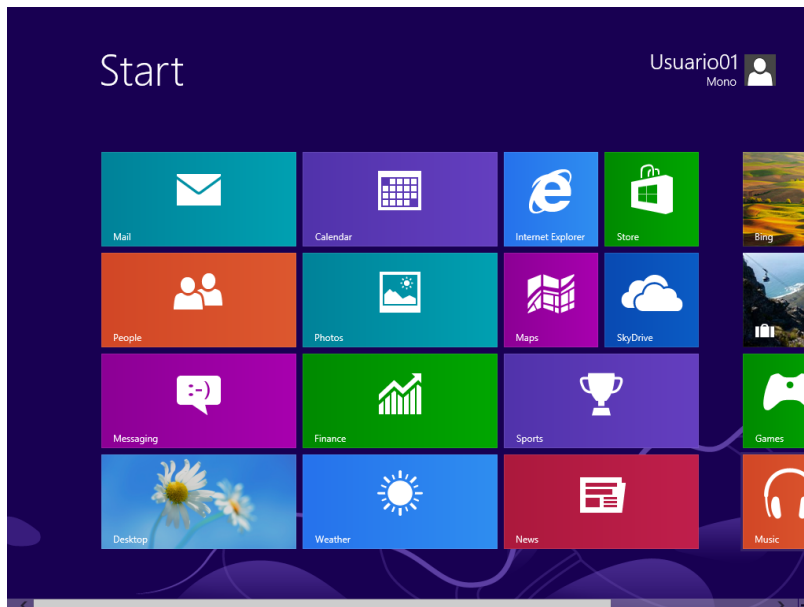
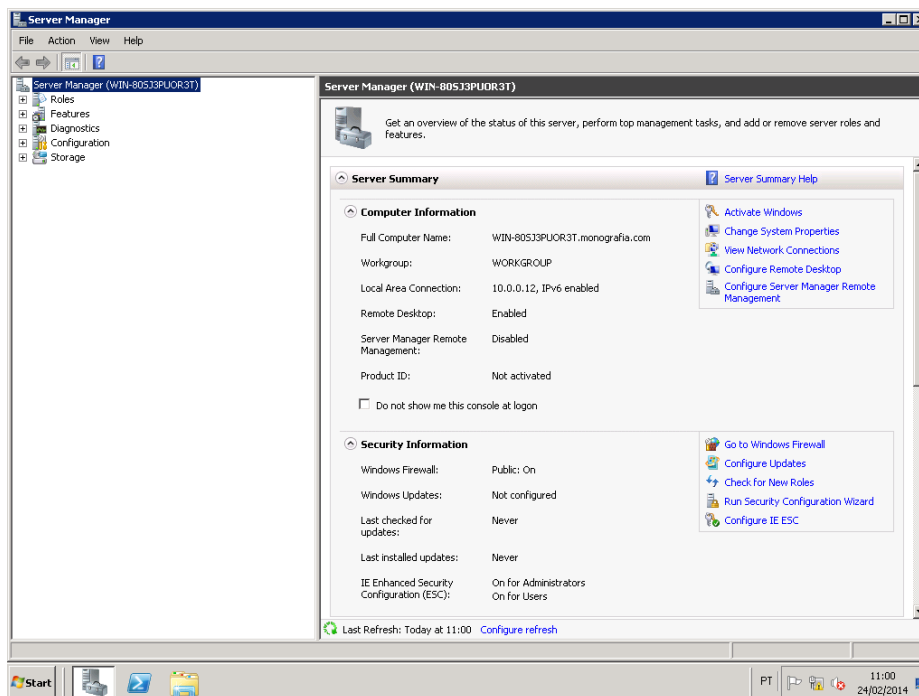


Figura 43 – Usuário Logado no Computador Cliente



Para incluir o servidor Windows Server 2008 R2 é preciso acessar com o usuário de administrador local, e abrir o gerenciador do servidor ou Server Manager e marcar o servidor local conforme abaixo:

Figura 44 – Gerencia do Servidor 2008 R2 para Arquivos



Depois de marcar o servidor local é preciso modificar as propriedades do sistema acessando o link Change System Properties.

Figura 45 – Propriedades do Sistema do Servidor de Arquivos

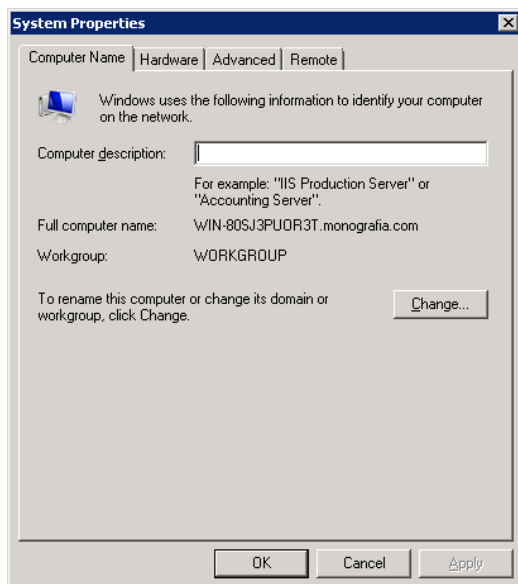
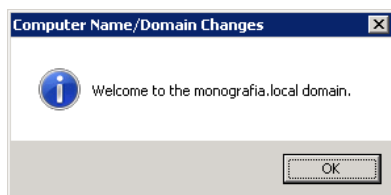


Figura 46 – Troca de Nome e Domínio do Servidor



Figura 47 – Confirmação de Alteração de Domínio para Monografia.local



5.1.8 Experimento 1 – Criação de Políticas de Segurança e Verificação dos resultados

As políticas de segurança que serão adotadas para experimento seguem algumas regras de segurança estabelecidas por políticas de segurança usadas em empresas de grande porte incluindo governo federal.

Os parâmetros de segurança usados neste experimento são:

Senha com complexidade

Acesso restrito a pastas

Existem duas procedimentos para definir a senha de segurança como complexa só para o grupo de suporte técnico. A primeira é modificando a política padrão do AD, que determina que todas as senhas tenham complexidade para que não seja mais uma exigência em seguida acessando criando uma política só para o

grupo de suporte técnico exigindo a complexidade de senha forçadamente. A Segunda opção é criar uma política que não exige senha complexa e atrelar a cada grupo criado menos aquele que terá a exigência mantendo a política padrão do AD. A primeira forma foi escolhida para o experimento devido ao menor esforço.

Figura 48 – Gerência de Política de Grupo

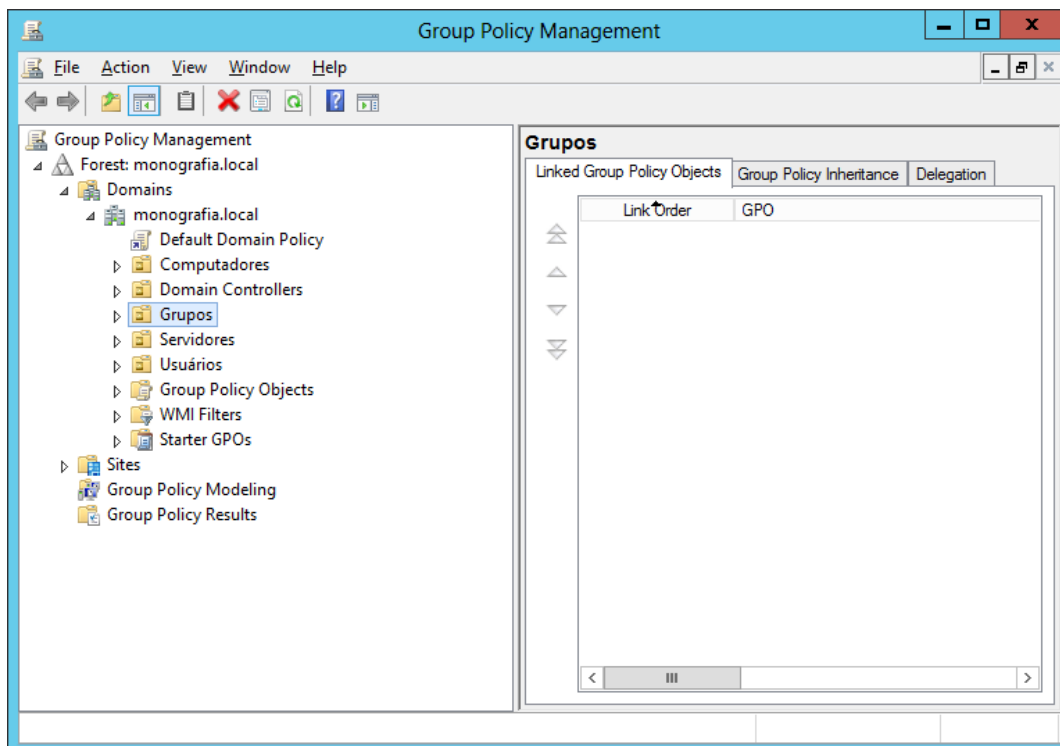


Figura 49 – Grupos Locais – GPO

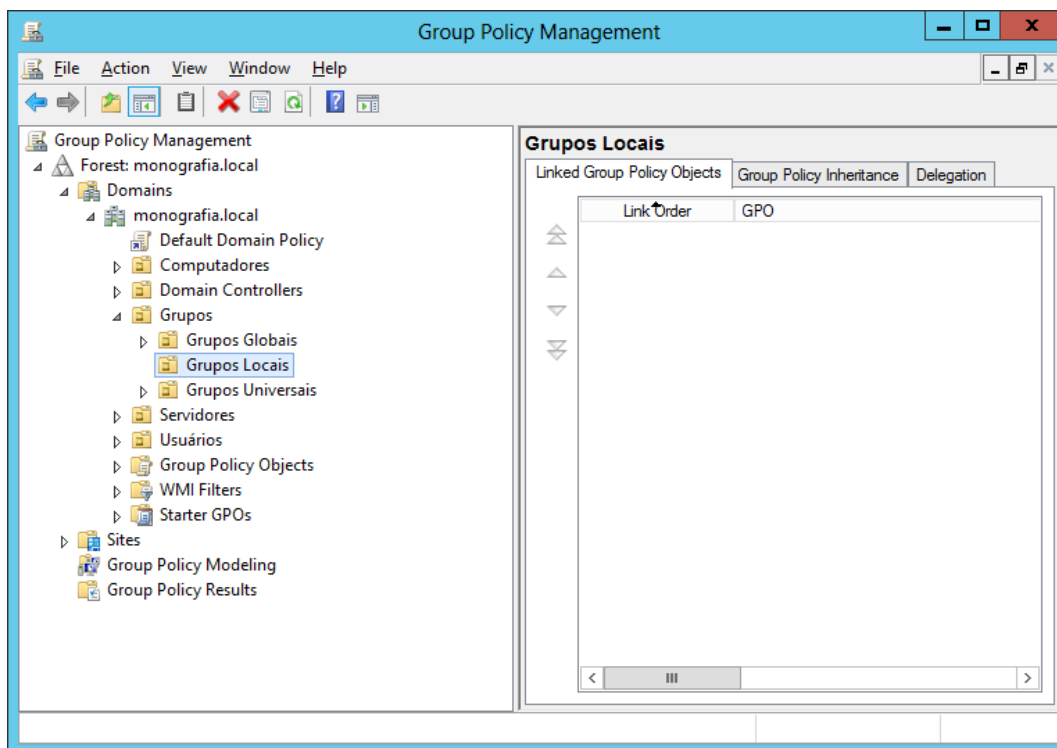


Figura 50 – GPO Senha Complexa

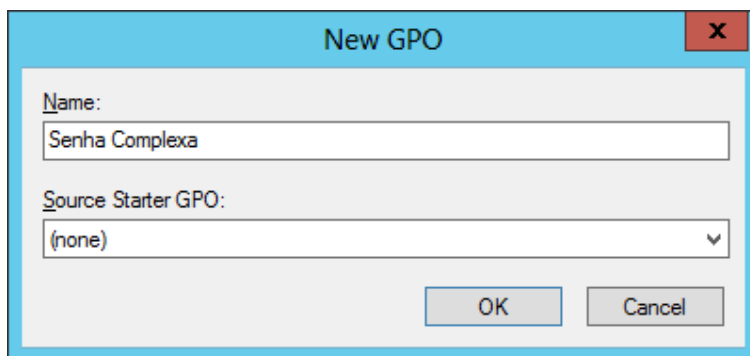


Figura 51 – GPOs no Grupo Local

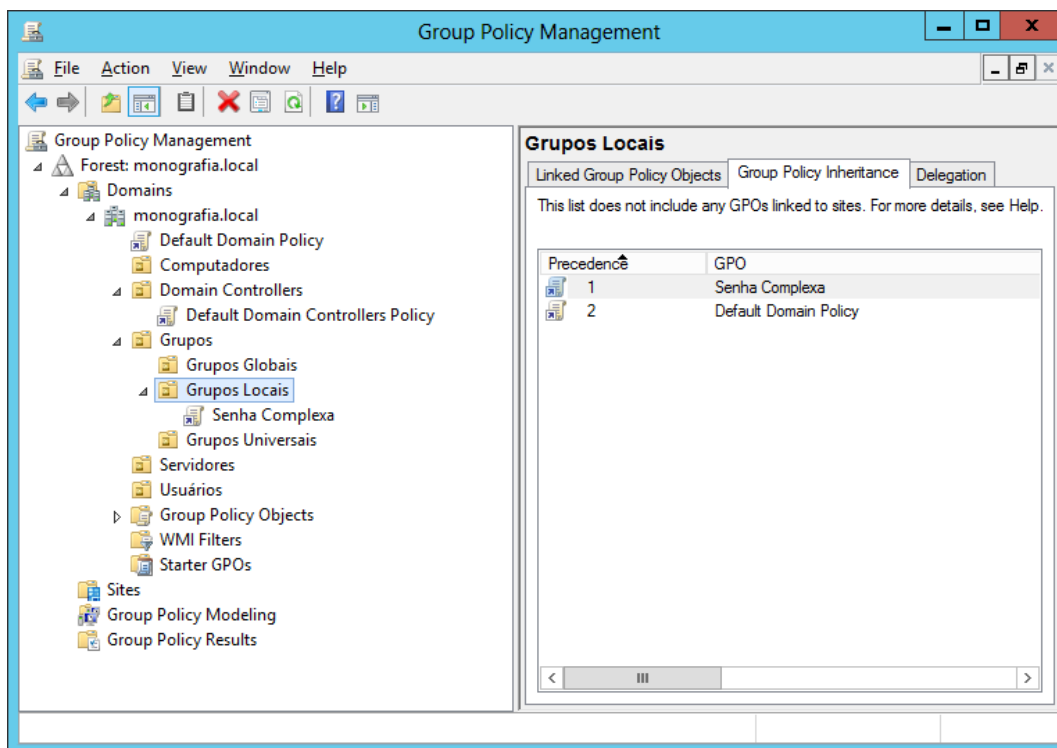


Figura 52 – Escopo da GPO Senha Complexa

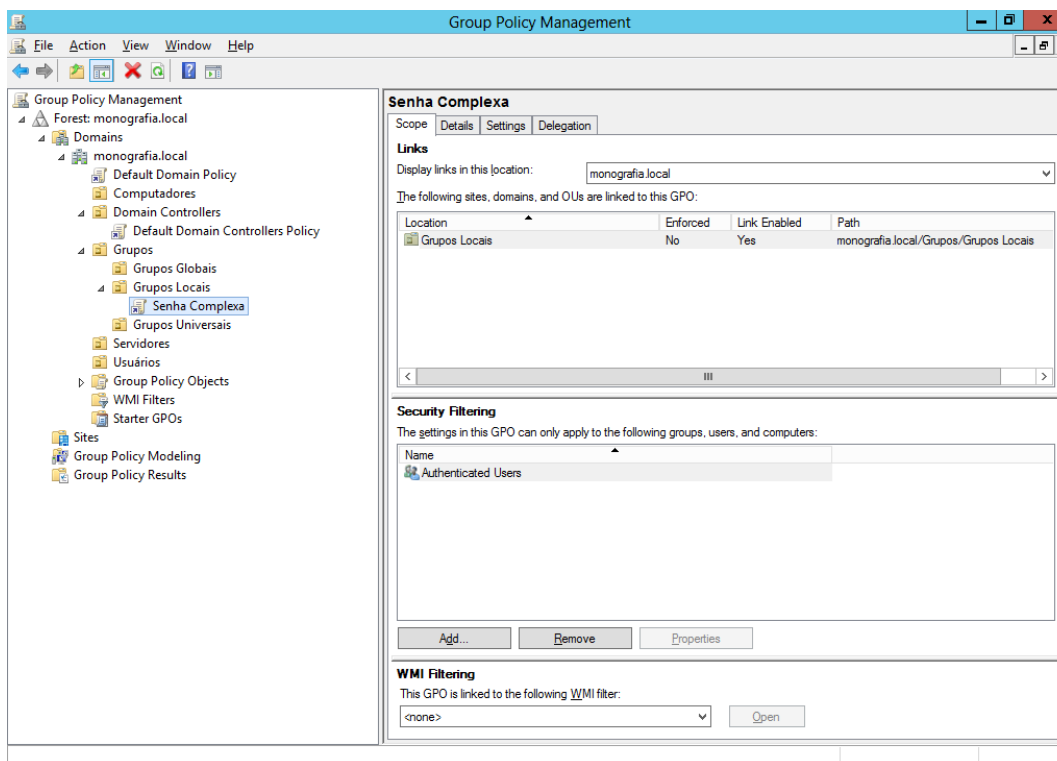


Figura 53 – Aba para Atribuir Permissão no Grupo

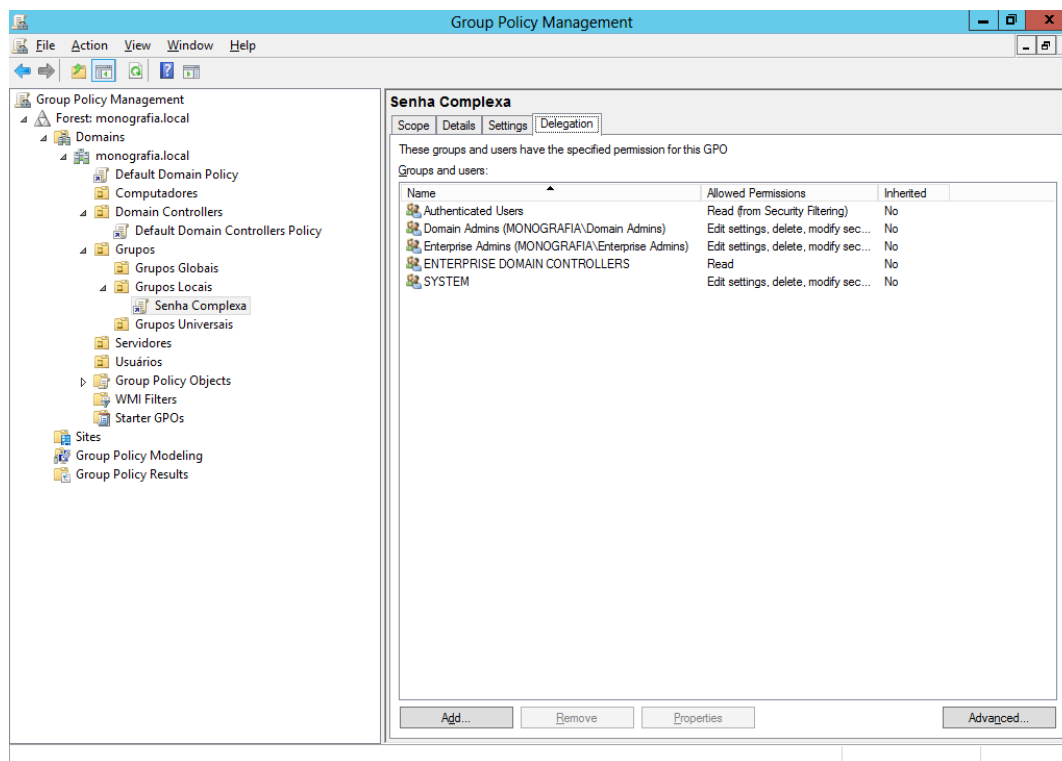


Figura 54 – Permissão para o Grupo Suporte Técnico

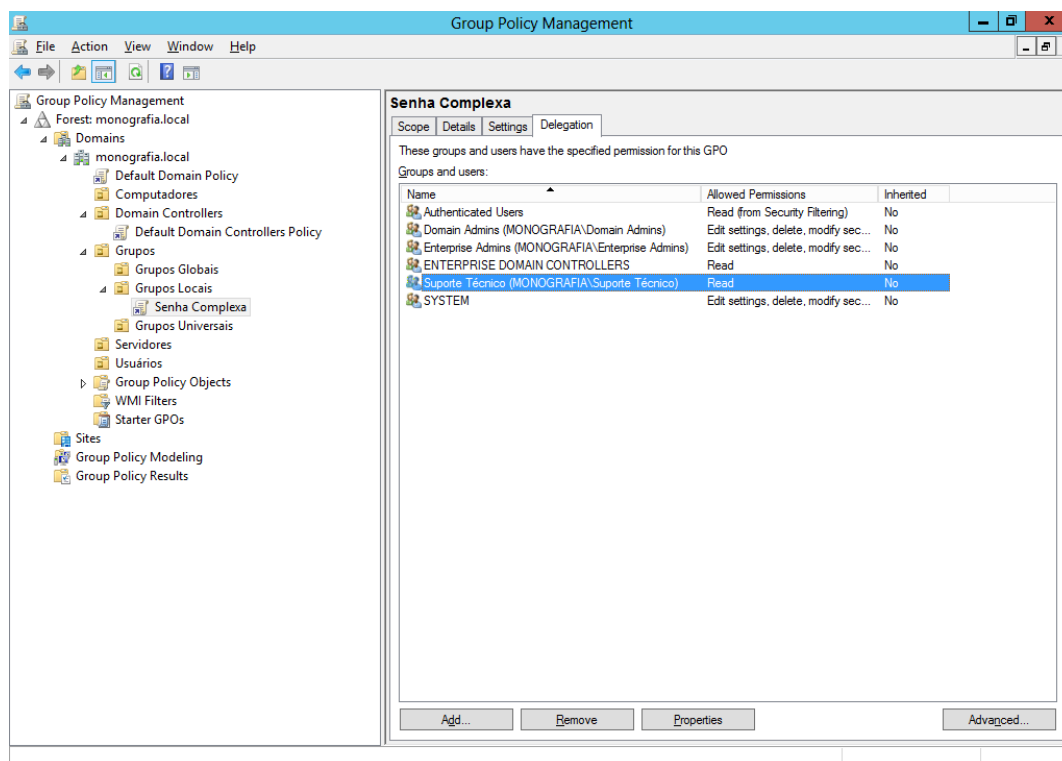


Figura 55 – Configurações de Segurança da GPO de Senha Complexa

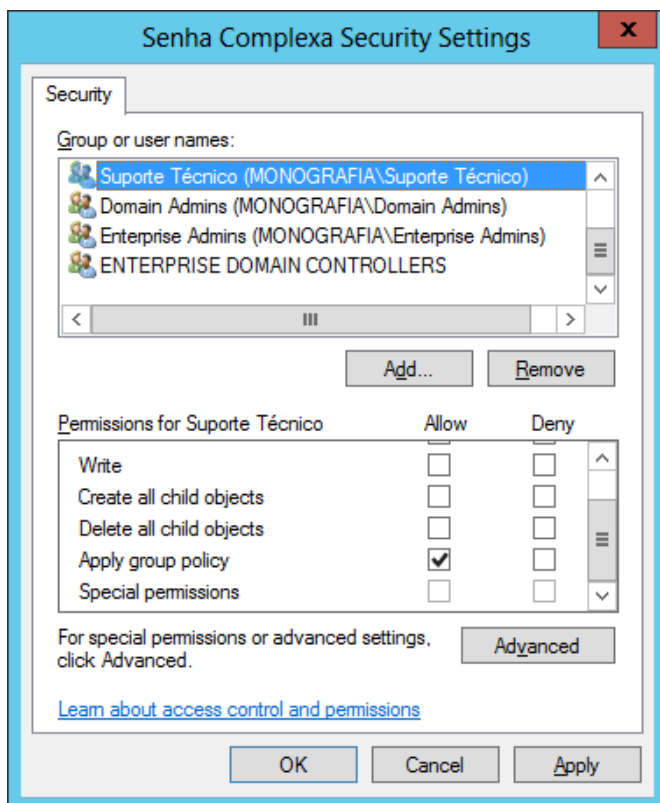
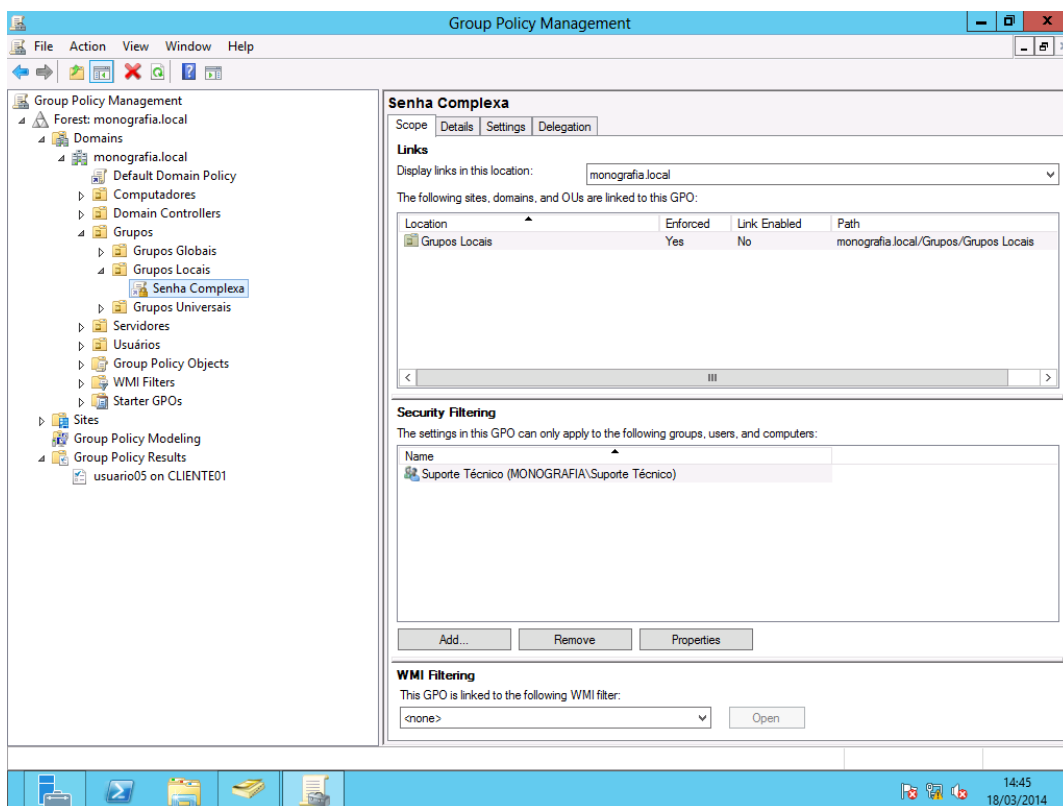


Figura 56 – Filtro de Segurança para Suporte Técnico



5.1.8.1 Editar

Ao editar a política de segurança padrão, todos os objetos do domínio são submetidos a nova regra geral. Permitindo que novas regras sejam criadas. Após a modificação da política padrão do AD foi criada a política de complexidade para o grupo alvo de experimento.

Figura 57 – Editor de GPO

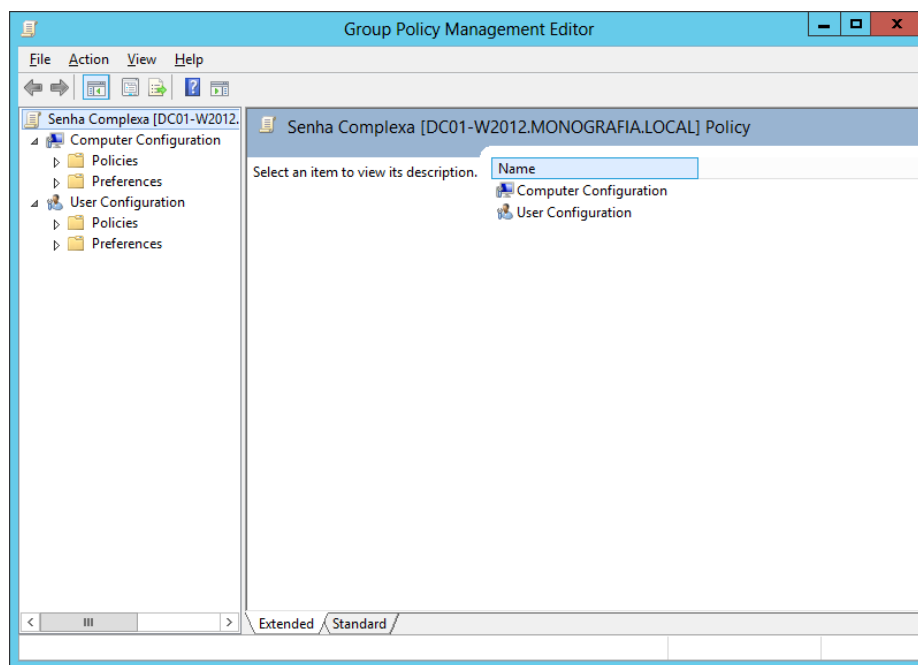


Figura 58 – Editor de Políticas de Contas

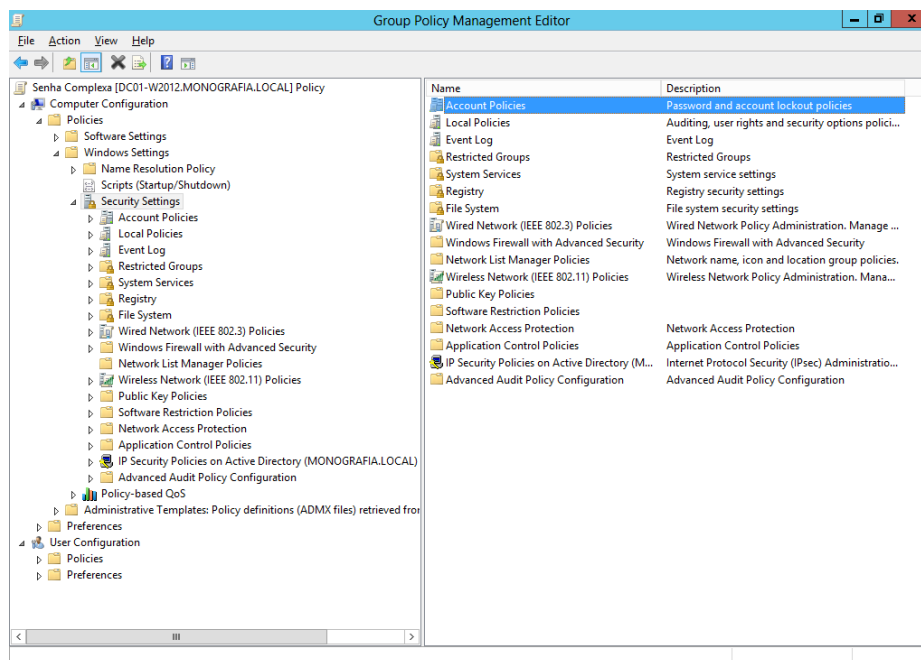


Figura 59 – Acesso à Política de Senhas da GPO

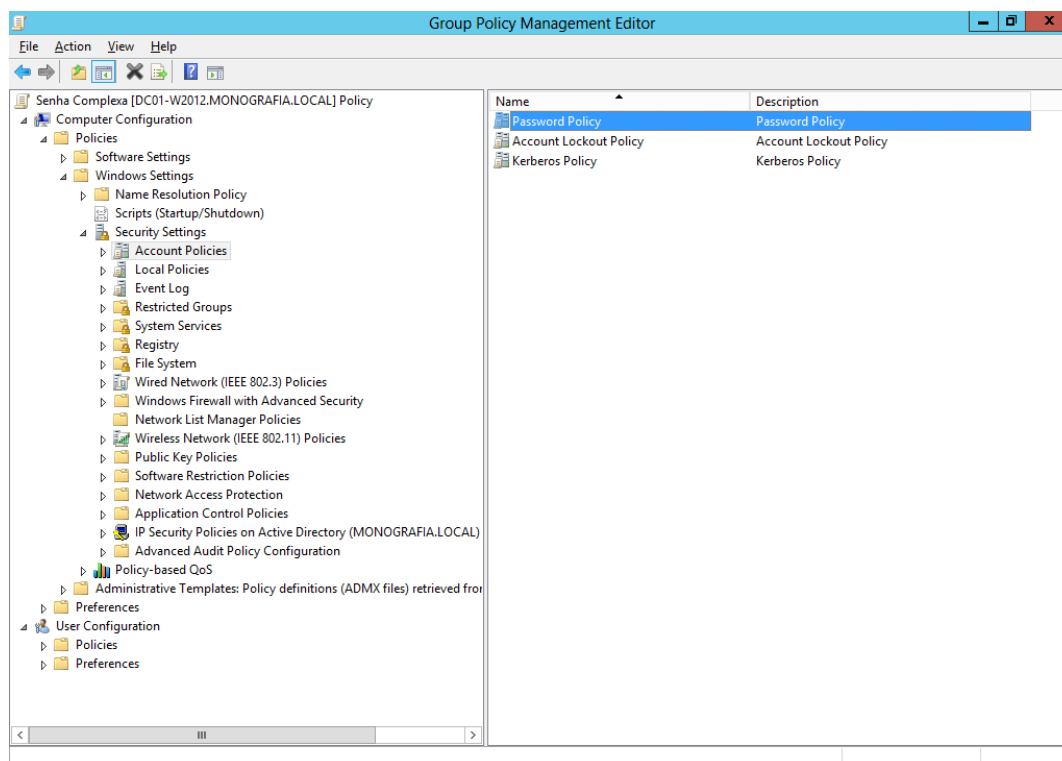


Figura 60 – Editando a Regra de Complexidade de Senhas

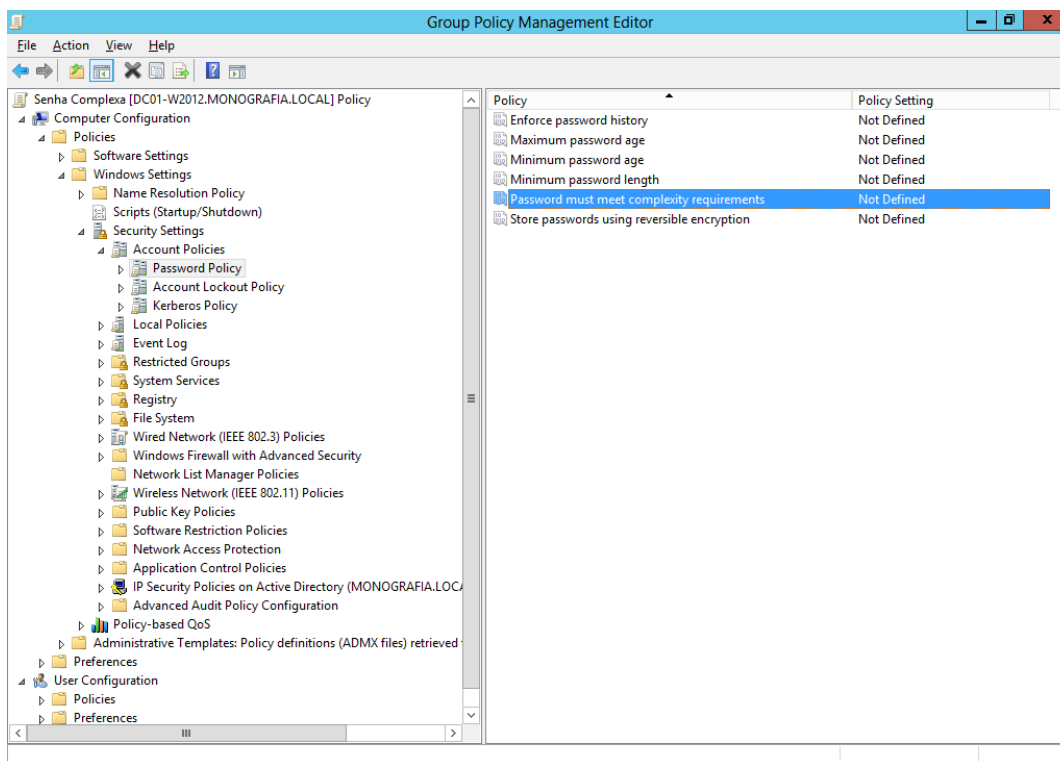
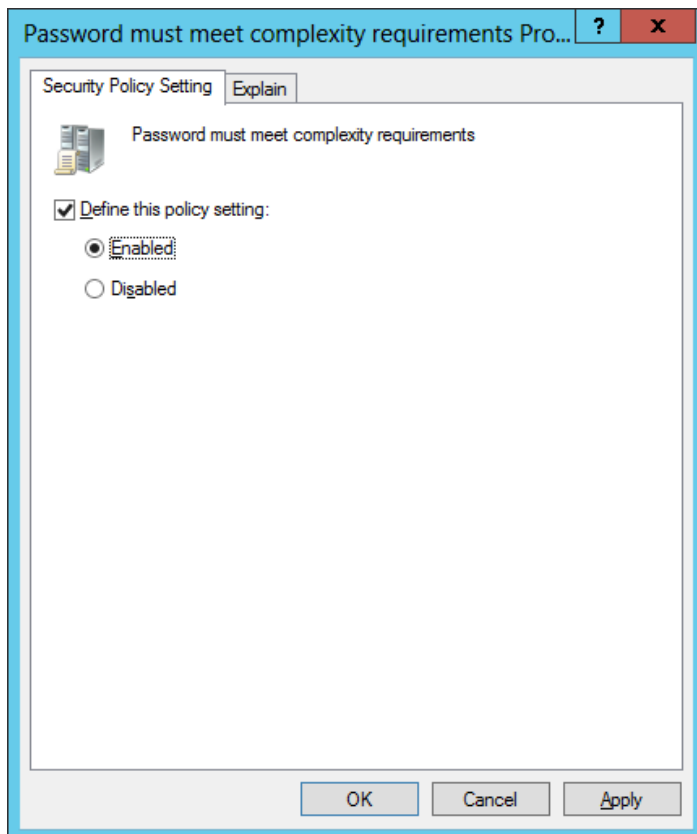


Figura 61 – Habilitando a Política de Complexidade de Senhas



5.1.8.2 Verificar a Política Aplicada

Ao utilizar um usuário que não faz parte do grupo suporte técnico, a política permitiu que o usuário trocasse a senha por uma sem complexidade com sucesso. O usuário usuario04 fez acesso a máquina Cliente01 com a senha sem complexidade 123456 quando questionado para modificar, a senha nova foi colocada sem complexidade, 654321 e Windows permitiu a mudança com sucesso.

Quando o usuario5 que faz parte do grupo de suporte foi questionado a modificar a senha, foi feito o teste de colocar uma senha sem complexidade, o Windows retornou a necessidade de colocar uma nova senha respeitando a política de complexidade. O teste foi realizado com sucesso provando a eficácia da política aplicada.

Abaixo segue as imagens das respostas do Windows durante os testes:

Figura 62 – Acesso do usuário no cliente

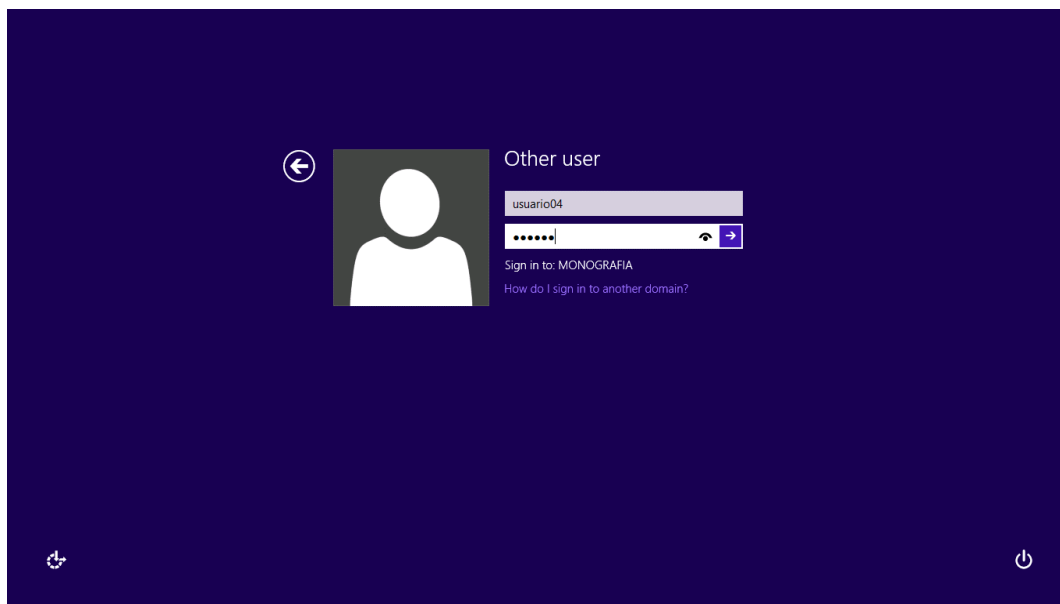


Figura 63 – A Senha Deve Ser Modificada

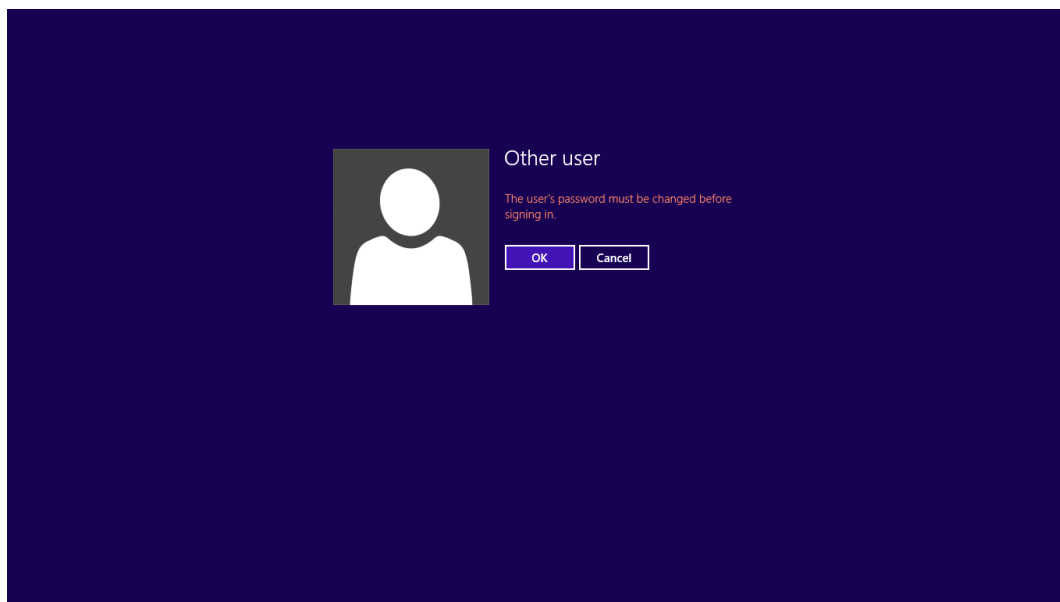


Figura 64 – Troca de Senha

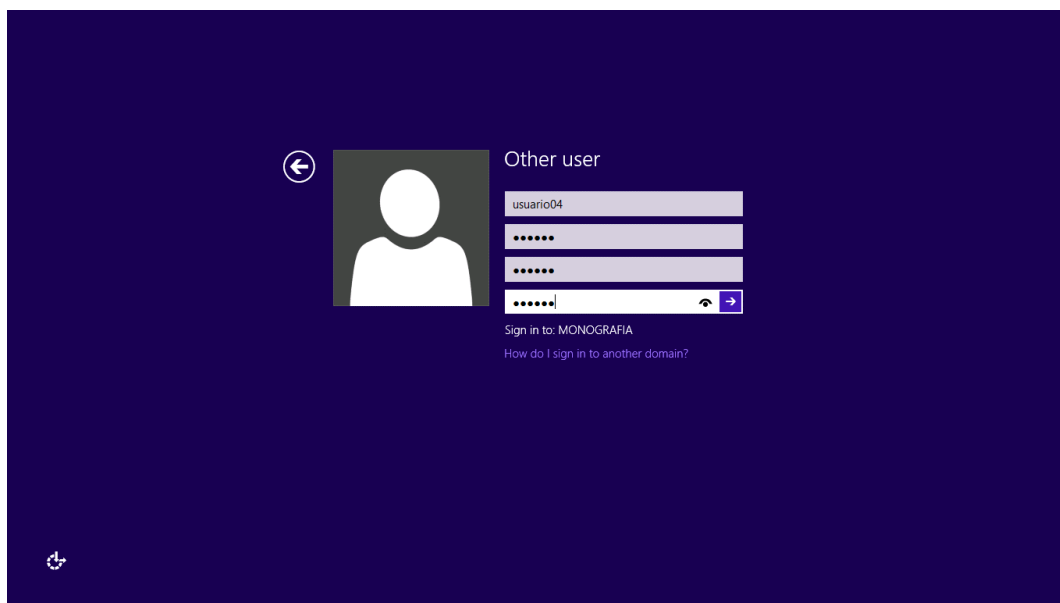


Figura 65 – Senha foi Modificada para Uma de Baixa Complexidade

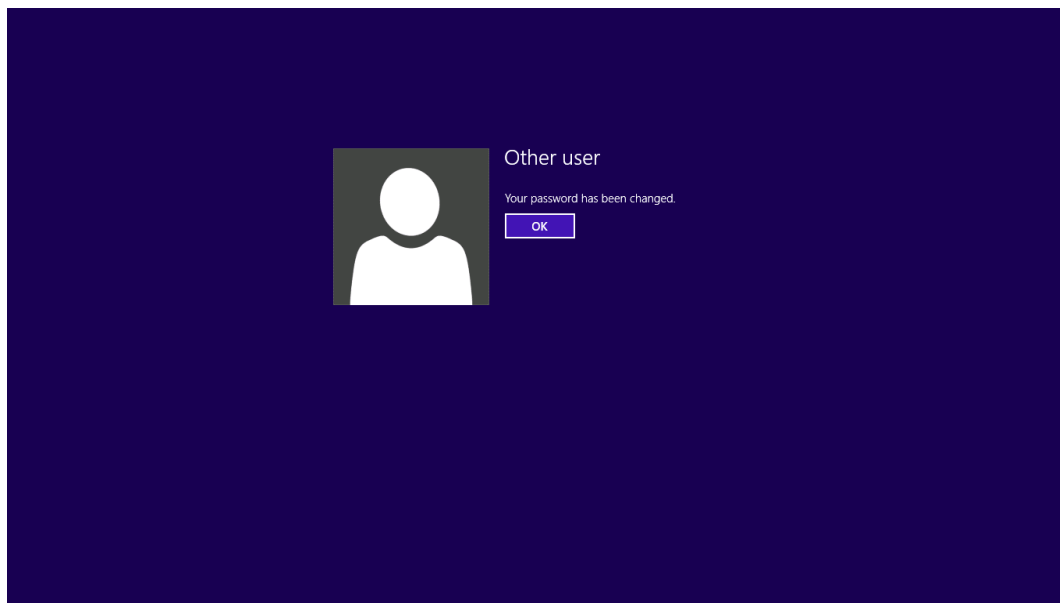


Figura 66 – Acesso do Usuário no Cliente

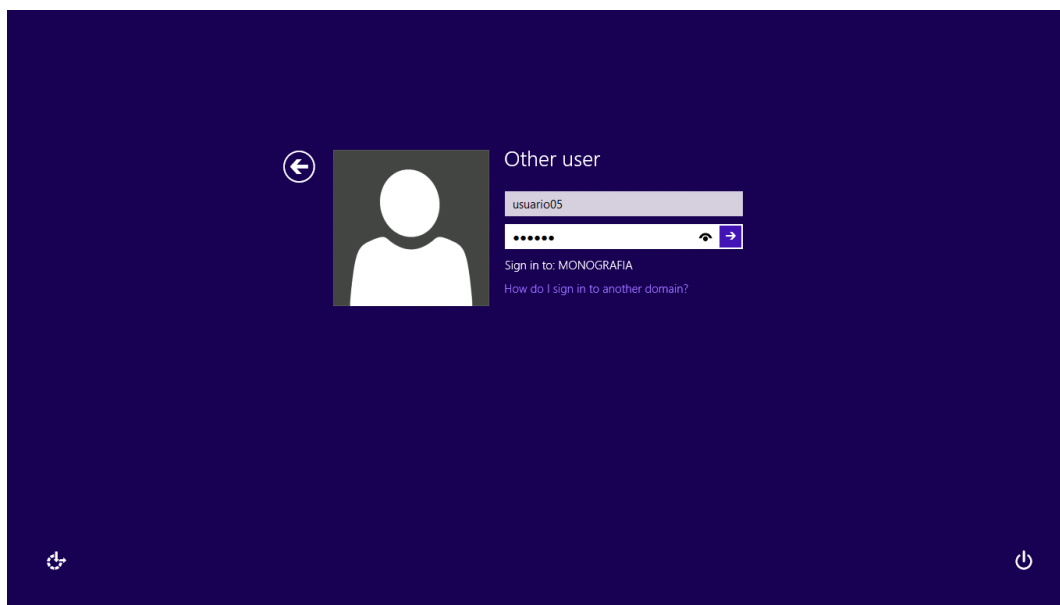


Figura 67 – A Senha deve Ser Modificada

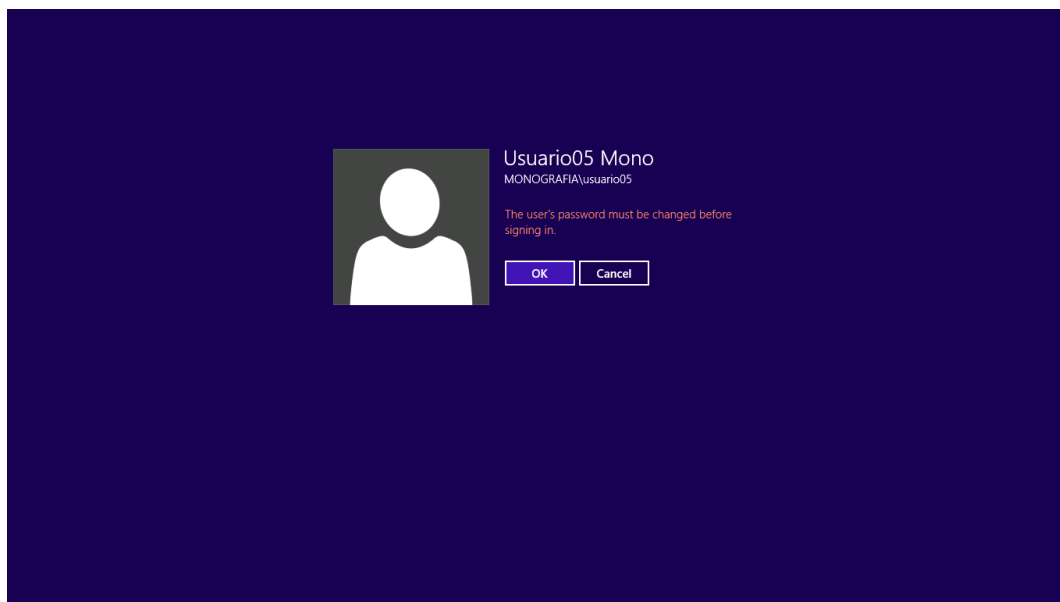


Figura 68 – Troca de Senha

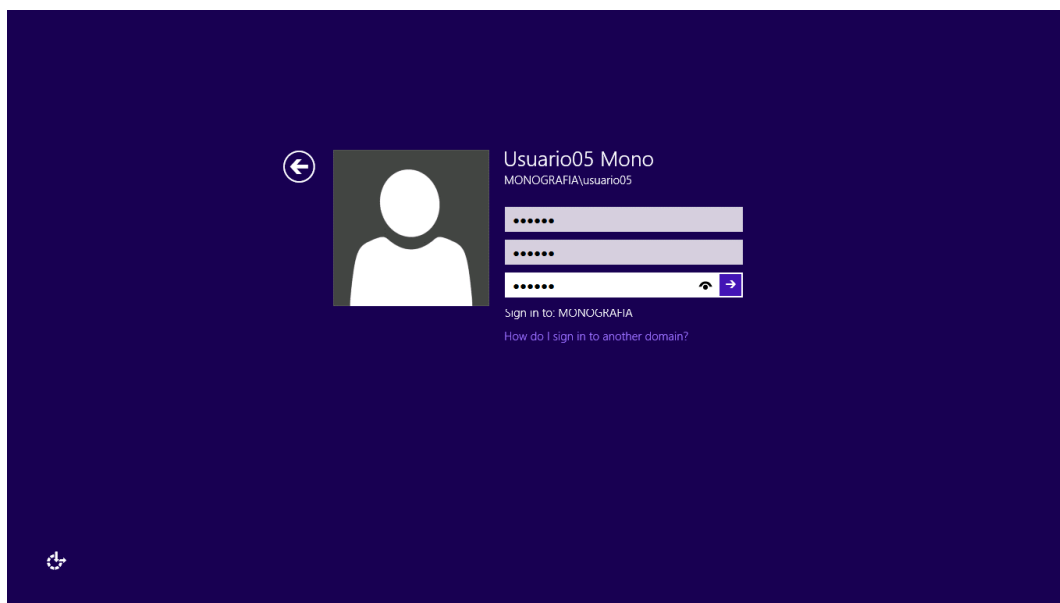


Figura 69 – Senha não Foi Modificada por ter Baixa Complexidade

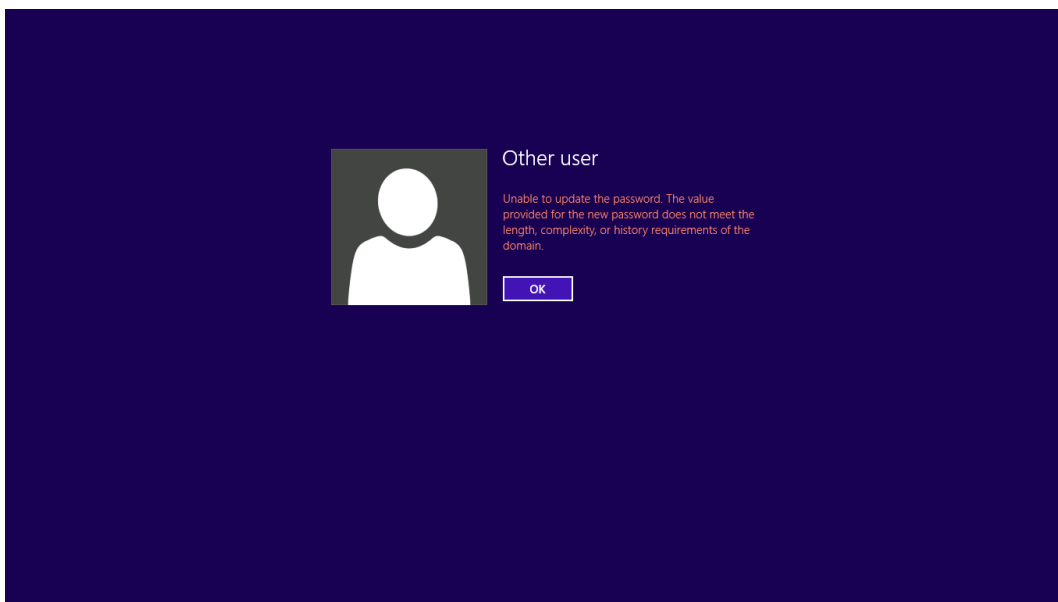
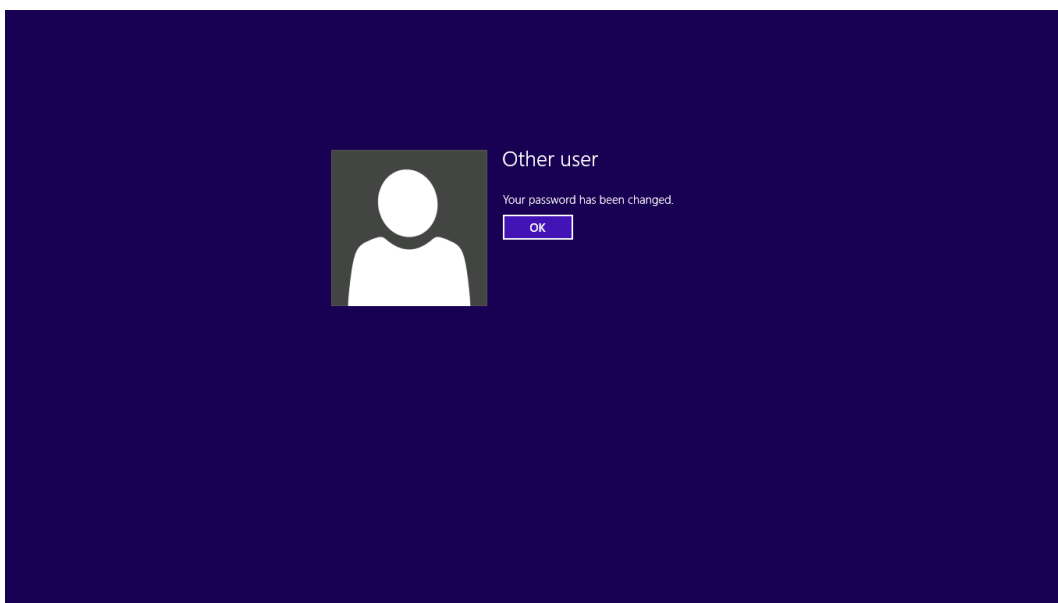


Figura 70 – Senha Modificada com Por Complexidade Alta



5.1.9 Experimento 2 – Criação de Política de Acesso em Pastas de Servidor de Arquivos e Verificar os Resultados.

Neste experimento foi usado um servidor de arquivos off-site, ou seja, o armazenamento de arquivos está localizado em outro servidor que não o AD. O

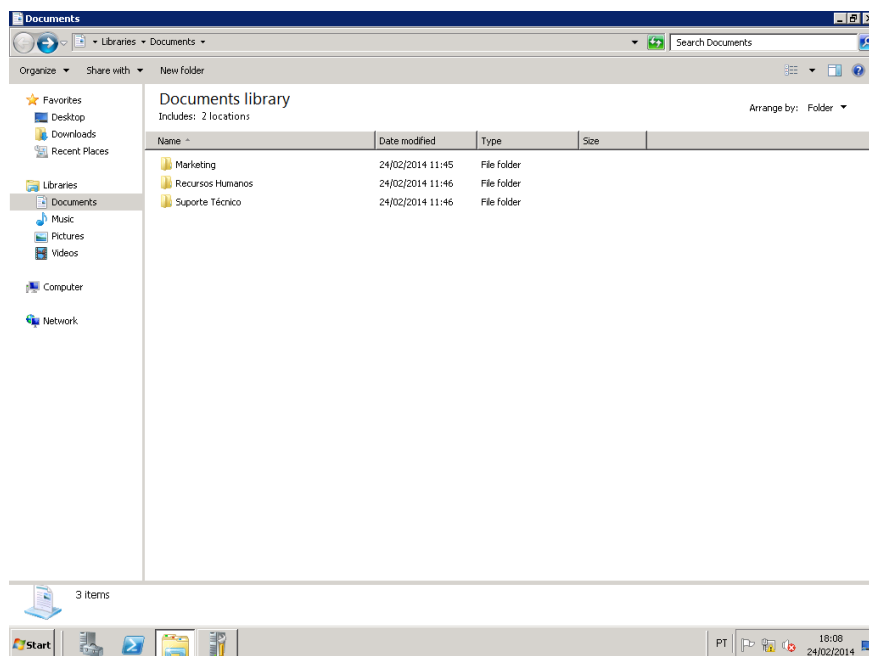
servidor usado neste experimento é um Windows Server 2008 R2 nomeado de Server01.

5.1.9.1 Criação de Pastas no Servidor de Arquivos

Para criar as pastas no servidor de arquivos basta acessar o servidor Server01 entrar em documentos e criar a pastas para salvar arquivos.

Para experimento foram criadas três pastas, Marketing, Recursos Humanos e Suporte Técnico, conforme figura abaixo.

Figura 71 – Pastas Criadas em Documentos



5.1.9.2 Criação da Política de Acesso às Pastas de Armazenamento de Arquivos

A política de acesso às pastas é feita através do compartilhamento na rede das mesmas, atribuindo permissões conforme o desejado pelo administrador.

No caso do experimento será dada permissão de acesso a pasta Marketing aos usuários pertencentes ao grupo Marketing, a pasta Recursos

Humanos ao grupo Recursos Humanos e a pasta Suporte Técnico ao grupo Suporte Técnico.

Para isso é preciso acessar a máquina Server01 e modificar as permissões de compartilhamento. O mesmo procedimento foi feito para todas as pastas e grupos respectivos.

Figura 72 –Acessando as Propriedades da Pasta

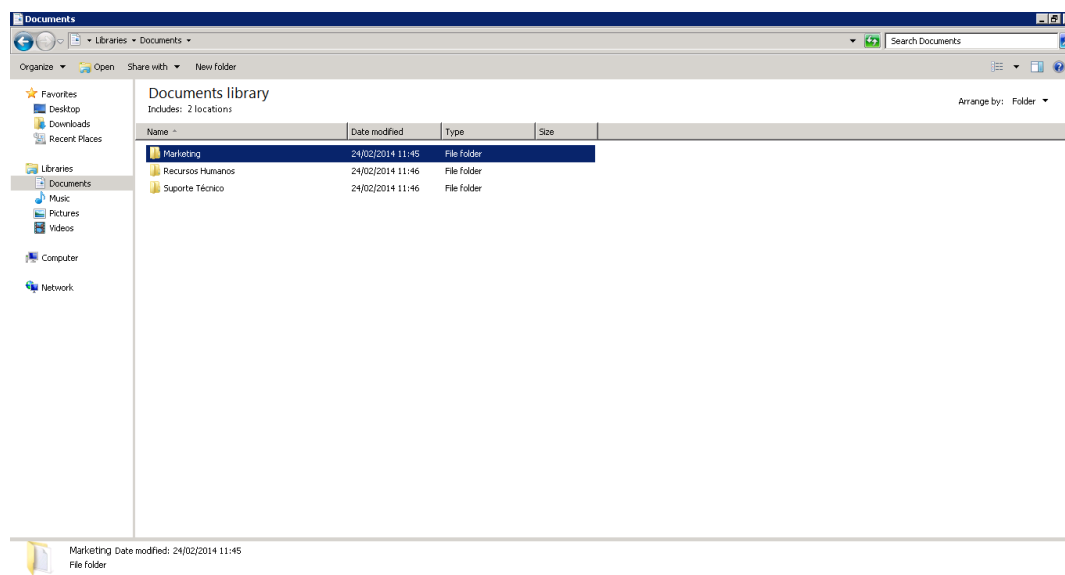


Figura 73 – Propriedades da Pasta

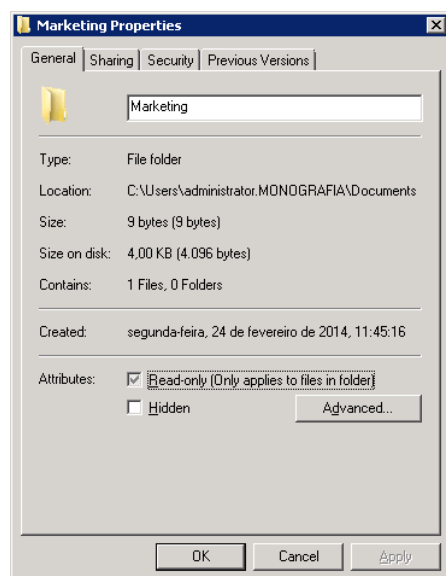


Figura 74 – Aba de Compartilhamento da Pasta

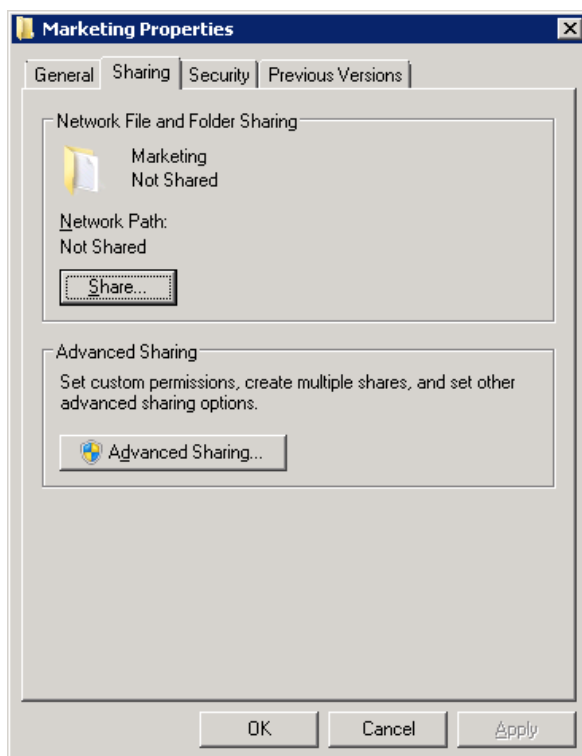


Figura 75 – Compartilhamento Avançado

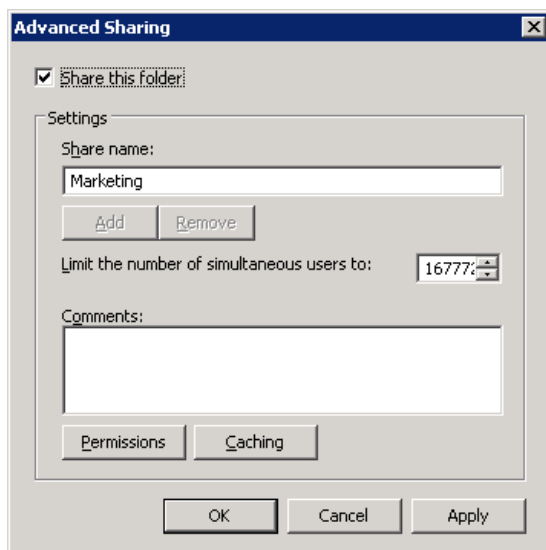


Figura 76 – Permissões de Acesso na Pasta

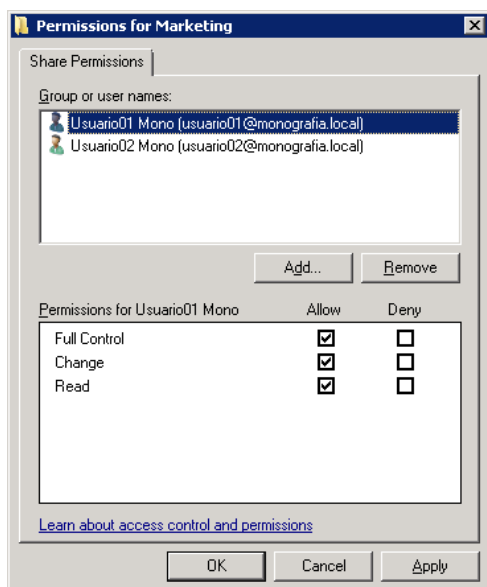


Figura 77 – Aba de Segurança de Acesso a Pasta

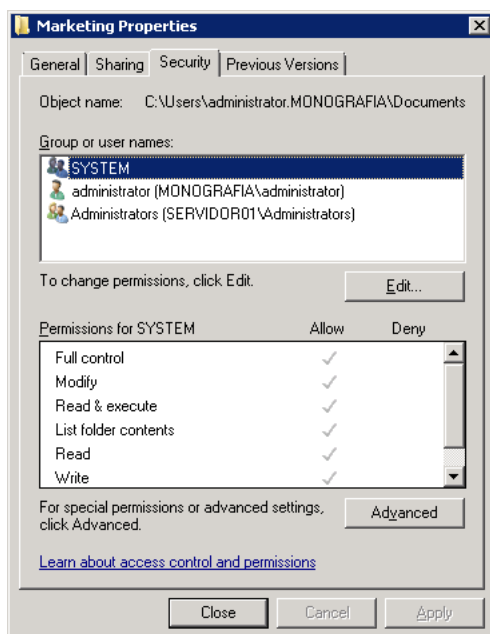
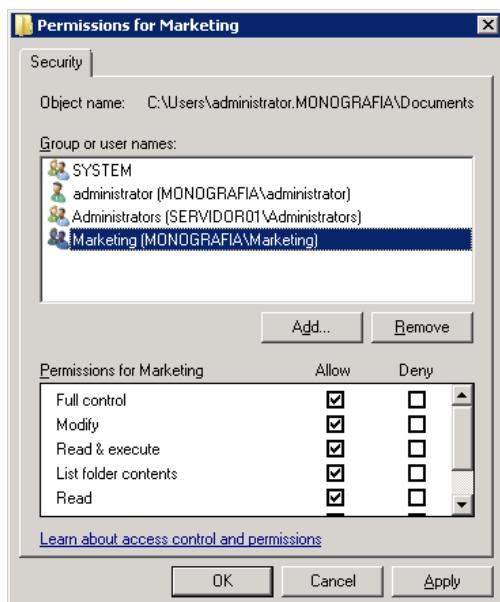


Figura 78 – Grupo com Acesso a Pasta



5.1.9.3 Verificação da Eficácia da Política de Acesso as Pastas

Verificação e teste da regra de segregação de pastas do servidor de arquivos.

Para fazer o teste é preciso acessar o computador cliente01, acessar a pasta correspondente ao grupo do usuário com sucesso e receber uma mensagem de acesso negado ao tentar acessar a pasta não correspondente ao grupo do usuário.

Acesso do usuário 1 a pasta correspondente:

Figura 79 – Credencias de Acesso

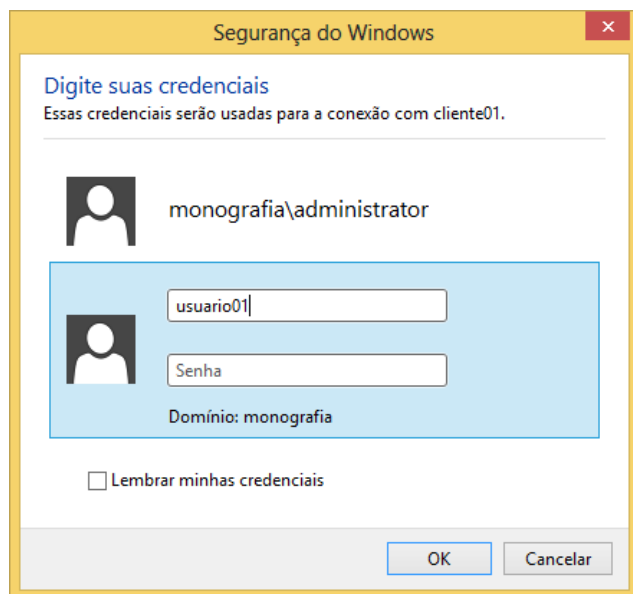
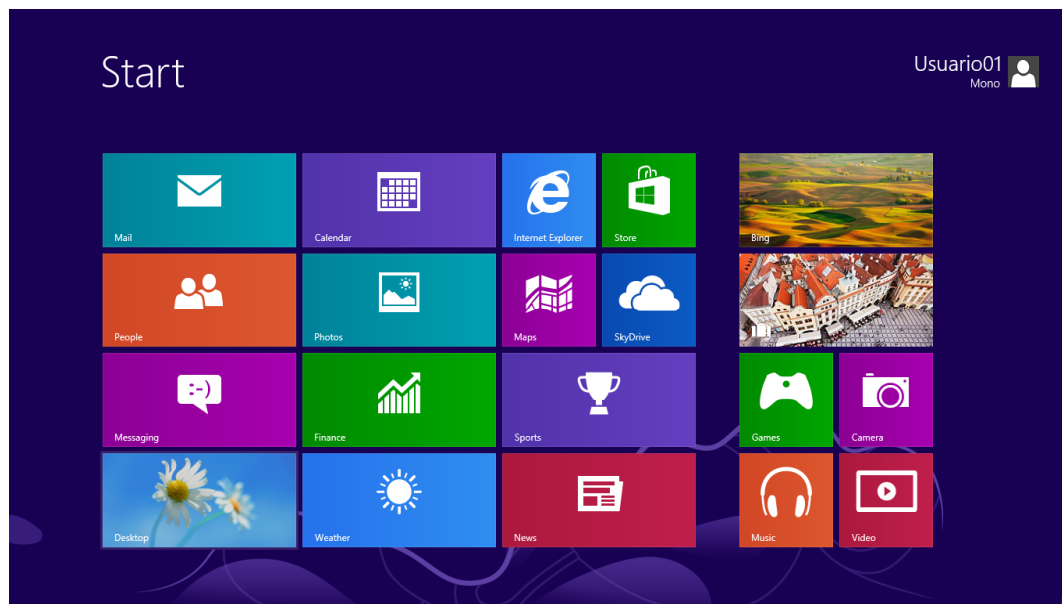
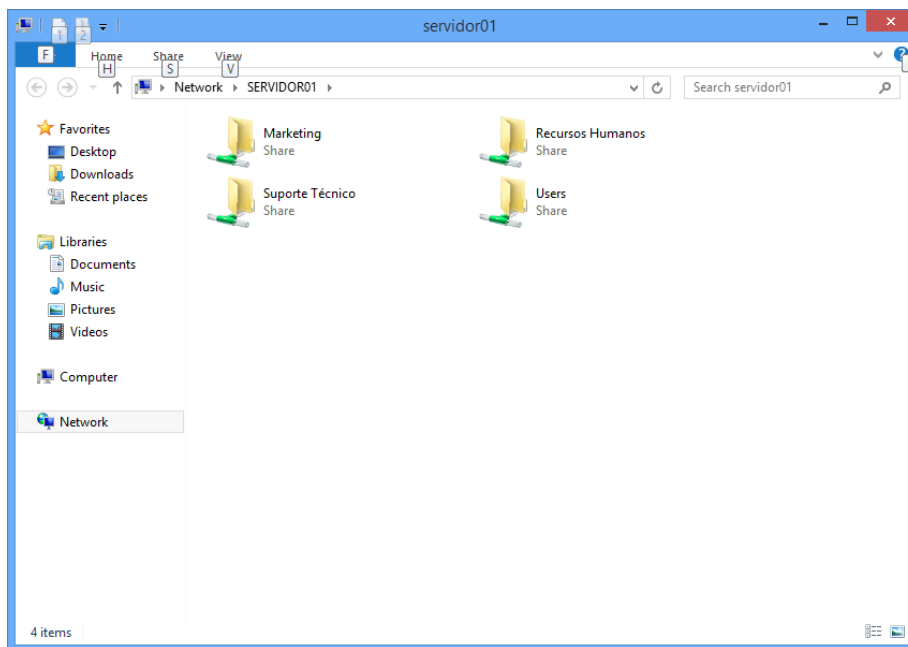


Figura 80 – Desktop do Cliente



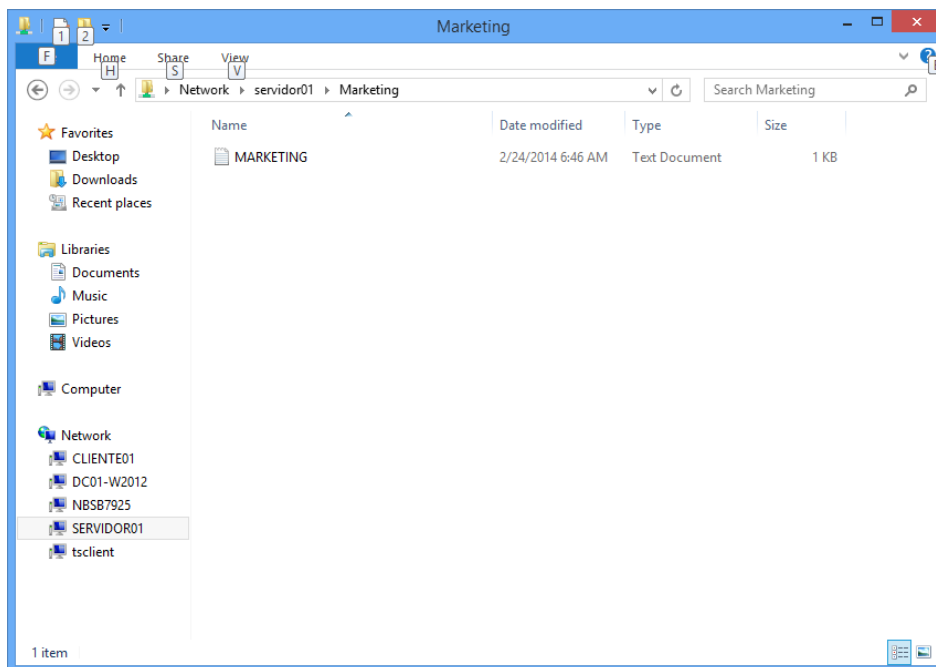
Para acessar a pasta compartilhada com a segurança é preciso acessar o servidor em que ela se encontra. No caso desse experimento o servidor de arquivos é o servidor01.

Figura 81 – Janela no Cliente, do Servidor, com as Pastas Criadas



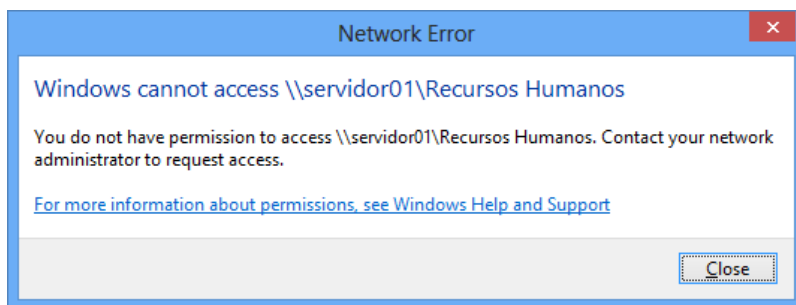
Ao acessar a pasta de Marketing, o usuário 1 tem acesso de controle total.

Figura 82 – Acesso Concedido ao Usuário na Pasta



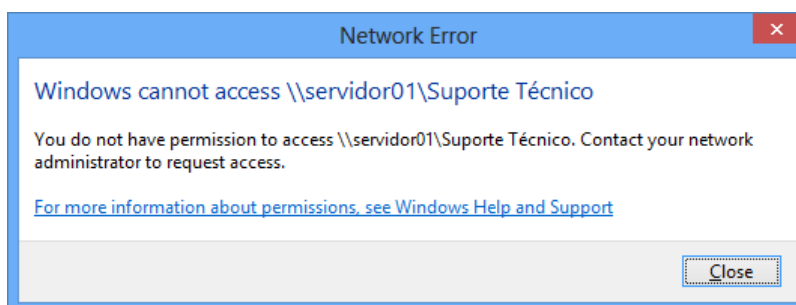
Ao tentar acessar a pasta de Recursos Humanos o usuário 1 recebe a seguinte mensagem:

Figura 83 – Acesso Negado ao Usuário na Pasta



E ao tentar acessar a pasta de suporte técnico o usuário 1 recebe a mesma mensagem:

Figura 84 – Acesso Negado ao Usuário na Pasta



O mesmo acontece com o usuário 2. Para os usuários 3 e 4 o mesmo acontece quando acessam a pasta de Recursos humanos e para os usuários 5 e 6 ao tentarem acesso à pasta Suporte Técnico.

5.2 Testes com o OpenLDAP

Para instalar o OpenLDAP é preciso ter um sistema operacional Linux instalado em uma máquina física ou virtual. Como o Linux tem um código de programação aberto, foram identificados vários tipos diferentes de Linux cada um deles descendente de um código fonte diferente com diferentes comandos, porém grande parte deles tem quase os mesmos comandos para operações simples.

Para este experimento foi escolhido por sua popularidade o sistema operacional Linux distribuição Ubuntu.

Inicialmente foi criada uma máquina virtual com parâmetros pré-determinados, para este teste específico com um ambiente relativamente pequeno,

onde existe um servidor de serviço de diretório responsável por fazer a autenticação centralizada para poucas máquinas no caso um máximo de duas máquinas.

O hardware-virtual da máquina foi configurado com os seguintes parâmetros:

- Processamento da máquina hospedeira no caso um CORE i5;
- 1024 Mb de memória RAM dinâmica, ou seja, é possível balancear o uso da memória do computador hospedeiro com outras aplicações, disponibilizando mais ou menos memória conforme necessário;
- 16 Gb de Armazenamento em disco rígido virtual;

Após a criação da máquina virtual foi obtido o programa do sistema operacional em que será instalado o programa OpenLDAP, neste caso, a distribuição Linux Ubuntu versão 13.10. Além de estar sendo indicado o uso pelo livro Mastering OpenLDAP de Matt Butcher.

É preciso fazer a atualização do sistema após a instalação usando os comandos:

Apt-get update

Apt-get dist-upgrade

Apt-get upgrade

Apt-get autoremove

Informação retirado do sítio: <http://www.ubuntubrsc.com/13-principais-comandos-do-ubuntu.html>.

Para transformar a distribuição Ubuntu, sistema Linux com base Debian, em um servidor de serviço de diretório é preciso instalar o OpenLDAP e o pacote slapd. Os clientes estão no pacote ldap-utils, e as bibliotecas estão empacotadas na versão mais nova do libldap. Quando o pacote libldap está desatualizado e uma instalação é feita, o próprio Linux sugere uma biblioteca mais nova, como na imagem abaixo:

Figura 85 – Falha na Instalação dos Pacotes

```

root@administrador-Virtual-Machine:/home/administrador# sudo apt-get install libldap-2.3-0 slapd ldap-utils
A ler as listas de pacotes... Pronto
A construir árvore de dependências
A ler a informação de estado... Pronto
O pacote libldap-2.3-0 não está disponível, mas é referenciado por outro pacote.
Isso pode significar que o pacote falta, ou ficou obsoleto, ou
está disponível somente a partir de outra fonte
No entanto, os seguintes pacotes substituem-no:
  libldap-2.4-2:i386 libldap-2.4-2
E: O pacote 'libldap-2.3-0' não tem candidato para instalação

```

Neste caso o comando teve que ser modificado para apt-get install libldap-2.4-2 slapd ldap-utils.

Figura 86 – Instalação do Pacote

```

root@administrador-Virtual-Machine:/home/administrador# sudo apt-get install libldap-2.4-2 slapd ldap-utils
A ler as listas de pacotes... Pronto
A construir árvore de dependências
A ler a informação de estado... Pronto
libldap-2.4-2 já está na versão mais recente.
Os seguintes pacotes extra serão instalados:
  libodbc1 libslp1
Pacotes sugeridos:
  libmyodbc odbc-postgresql tdsodbc unixodbc-bin slpd openssl-doc
Serão instalados os seguintes NOVOS pacotes:
  ldap-utils libodbc1 libslp1 slapd
0 pacotes actualizados, 4 pacotes novos instalados, 0 a remover e 0 não actualizados.
É necessário obter 2.294 kB de arquivos.
Após esta operação, serão utilizados 5.639 kB adicionais de espaço em disco.
Deseja continuar [Y/n]?

```

Figura 87 – Pacotes Instalados

```

Após esta operação, serão utilizados 5.639 kB adicionais de espaço em disco.
Deseja continuar [Y/n]? y
Obter:1 http://br.archive.ubuntu.com/ubuntu/ saucy/main libodbc1 amd64 2.2.14p2-5ubuntu4 [226 kB]
Obter:2 http://br.archive.ubuntu.com/ubuntu/ saucy/main libslp1 amd64 1.2.1-9 [45,1 kB]
Obter:3 http://br.archive.ubuntu.com/ubuntu/ saucy/main slapd amd64 2.4.31-1+nmu2ubuntu3 [1.738 kB]
Obter:4 http://br.archive.ubuntu.com/ubuntu/ saucy/main ldap-utils amd64 2.4.31-1+nmu2ubuntu3 [285 kB]
Obtidos 2.294 kB em 3s (651 kB/s)
A pré-configurar os pacotes...
A seleccionar pacote anteriormente não seleccionado libodbc1:amd64.
(A ler a base de dados ... 193041 ficheiros e directórios actualmente instalados.)
A descompactar libodbc1:amd64 (desde .../libodbc1_2.2.14p2-5ubuntu4_amd64.deb) ...
A seleccionar pacote anteriormente não seleccionado libslp1.
A descompactar libslp1 (desde .../libslp1_1.2.1-9_amd64.deb) ...
A seleccionar pacote anteriormente não seleccionado slapd.
A descompactar slapd (desde .../slapd_2.4.31-1+nmu2ubuntu3_amd64.deb) ...
A seleccionar pacote anteriormente não seleccionado ldap-utils.
A descompactar ldap-utils (desde .../ldap-utils_2.4.31-1+nmu2ubuntu3_amd64.deb) ...
A processar 'triggers' para man-db ...
A processar 'triggers' para ufw ...
A processar 'triggers' para ureadahead ...
ureadahead will be reprofiled on next reboot
A instalar libodbc1:amd64 (2.2.14p2-5ubuntu4) ...
A instalar libslp1 (1.2.1-9) ...
A instalar slapd (2.4.31-1+nmu2ubuntu3) ...
  Creating new user openldap... done.
  Creating initial configuration... done.
  Creating LDAP directory... done.
* Starting OpenLDAP slapd
A instalar ldap-utils (2.4.31-1+nmu2ubuntu3) ...
A processar 'triggers' para libc-bin ...
A processar 'triggers' para ufw ...
A processar 'triggers' para ureadahead ...
root@administrador-Virtual-Machine:/home/administrador#

```

Durante a instalação dos pacotes o usuário é questionado quanto a senha do usuário que será o administrador do serviço de diretório, em seguida o OpenLDAP está instalado.

De acordo com o livro Mastering OpenLDAP de Matt Butcher é preciso fazer o backup do slapd.conf, arquivo de configuração do diretório que vem pré-configurado e criar um novo arquivo com o mesmo nome, porém, ao tentar localizar o arquivo, o Ubuntu informa que o arquivo não pode ser localizado.

Após esse erro, que de acordo com alguns sites está com o nome do arquivo desatualizado, foi feita a instalação do OpenLdap usando as informações do site oficial do OpenLDAP, porém, um erro de configuração de pré-requisitos para instalação é apresentado. Após varias tentativas de criar um laboratório com o OpenLDAP sem sucesso. Foi decidido então procurar um ambiente que já tem o sistema configurado para fazer os testes propostos nesse trabalho.

O primeiro desafio proposto tanto para o sistema Windows como para o sistema Linux é criar um banco de dados de usuários que possam ser consultados oferecendo o serviço de diretório.

O segundo desafio é restringir acesso de usuários a um arquivo ou pasta, levando em conta a segurança.

O terceiro desafio é forçar que cada usuário, para fazer acesso no domínio criado, tenha senha com nível de complexidade específico dependendo do privilegio do usuário.

5.2.1 Criar um domínio com um banco de usuários

De acordo com o *site* oficial do OpenLDAP para instalar o software é preciso primeiro fazer o *download* no próprio *site* da ultima versão e descompacta-lo usando o seguinte comando:

```
gunzip -c openldap-VERSION.tgz | tar xvfB -
```

Onde openldap-VERSION.tgz deve ser substituído pelo nome da ultima versão do programa. Em é necessário entrar no diretório criado com a descompactação, usando o comando:

```
cd openldap-VERSION
```

Em seguida de entrar no diretório é preciso rodar o *script configure* que é fornecido no pacote OpenLDAP para construir a distribuição na máquina. O *script*

configure suporta vários outros comandos que habilitam ou desabilitam outras funcionalidades do sistema. O comando abaixo deve ser usado:

./configure (O comando “./configure --help” mostra outras funcionalidades que podem ser configuradas com outros comandos)

Para de construir o software é precisa usar dois comandos:

make depend

make

O passo seguinte é instalar o programa, usando o comando:

su root -c 'make install'

O comando “su” é usado para aumentar os privilégios do administrador.

Para criar o domínio é preciso editar o arquivo de configuração usando qualquer editor de arquivos para editar o arquivo *slapd.conf* para conter uma definição de banco de dados “BDB” no seguinte formato:

```
database bdb
suffix "dc=<MY-DOMAIN>,dc=<COM>"
rootdn "cn=Manager,dc=<MY-DOMAIN>,dc=<COM>"
rootpw secret
directory /usr/local/var/openldap-data
```

Neste caso é preciso substituir o “MY-DOMAIN” pelo nome do novo domínio, o domínio sugerido pelo site é *exemple.com*. A edição ficaria:

```
database bdb
suffix "dc=exemple,dc=COM"
rootdn "cn=Manager,dc=exemple,dc=com"
rootpw secret
directory /usr/local/var/openldap-data
```

Para iniciar o servidor é preciso iniciar o Standalone LDAP Daemon, *slapd*, usando o comando:

su root -c /usr/local/libexec/slapd

De acordo com o site nesse momento o serviço de diretório está funcional, o próximo passo é adicionar novas entradas no diretório.

Para adicionar novas entradas no diretório é preciso criar um arquivo com extensão LDIF e rodar o comando “*ldapadd*”.

Para criar a nova entrada é preciso abrir o arquivo LDIF com o editor de texto e completa-lo com alguns detalhes principais:

dn: dc=<MY-DOMAIN>,dc=<COM>

objectclass: dcObject

objectclass: organization

o: <MY ORGANIZATION>

dc: <MY-DOMAIN>

dn: cn=Manager,dc=<MY-DOMAIN>,dc=<COM>

objectclass: organizationalRole

cn: Manager

Após mudar os valores que estão entre os símbolos “<” e “>” o banco de dados do diretório tem o primeiro membro.

Com esses usuários no domínio pode-se acessar a maquina fazendo uma autenticação no banco de dados do diretório.

Porém o OpenLDAP é uma ferramenta que controla somente a autenticação de usuários, podendo fazer o controle dos usuários para acessar serviços usando listas de controle de acesso. Para fazer o controle de acesso a pastas e arquivos é preciso usar outro programa chamado SAMBA.

5.2.2 Por que SAMBA?

Em um ambiente de redes ideal, todos os computadores deveriam ser do mesmo fabricante, ter o mesmo sistema operacional, usar o mesmo protocolo de comunicação, ou seja, todos os equipamentos deveriam ser preparados pela mesma empresa para se comunicarem perfeitamente uns com os outros. Isso não é o que acontece. Hoje existem centenas de equipamentos que fazem a mesma coisa, que se comunicam por protocolos diferentes, tem fabricantes diferentes, formas diferentes, quase tudo diferente, porém, todos eles se comunicam entre si e realizam as funções que foram criados para realizar.

Usando esse pensamento e trazendo para a realidade, quase todas as empresas tem ambientes mistos, com equipamentos de diferentes fabricantes, sistemas operacionais diversos, e milhões de ferramentas de operação. O Samba é uma ferramenta que consegue fazer o gerenciamento de diretório, compartilhamento de arquivos, entre outras várias funcionalidades, entre a maioria, quase totalidade, dos sistemas operacionais do mundo.

O Samba implementa o protocolo de rede CIFS (Common Internet File System). Usando esse protocolo, o Samba permite que computadores com sistemas operacionais baseados no UNIX como, Linux, FreeBSD, CentOS, Solaris e OS X, se comuniquem com o Windows da Microsoft ou qualquer outro sistema que utilize o protocolo CIFS, seja ele um cliente ou um servidor. (CARTER, 2007)

Para este trabalho a forma genérica é a melhor opção, devido os ambientes de rede terem máquinas Microsoft e Unix.

5.2.3 Testes Samba

Para iniciar um serviço de diretório usando o SAMBA é preciso ter um IP estático para que sempre que o IP for consultado ele tenha um dono. Nesse experimento o IP do SAMBA é 192.168.1.100 em um Ubuntu Server 14.04 e o IP de uma estação de trabalho é 192.168.1.110 usando o Windows 8.1.

Também é preciso ter certeza de que o nome do servidor está correto porque após a instalação do serviço de diretório não será mais possível modificá-lo, nesse caso o servidor se chamará *ubuntuserver*.

5.2.3.1 Instalação do Ubuntu Server 14.04

Para fazer a instalação do Ubuntu Server foi criada uma máquina virtual no Hyper-V, ferramenta de virtualização do Windows para simular uma rede. É preciso entrar no site oficial do Ubuntu, <http://www.ubuntu.com/download/server>, para fazer o download do sistema operacional.

Uma vez com o sistema operacional é preciso inicia-lo na máquina virtual.

Em um primeiro momento é preciso escolher a língua que terá o servidor Ubuntu.

Figura 88 – Idioma do Sistema



Após a escolha de língua o Ubuntu se apresenta interativo, questionando quanto as ações a serem tomadas, por exemplo questionando se o disco do sistema deve ser usado para criar um novo servidor. Em seguida questionando quanto a língua do sistema e a língua padrão do teclado.

Figura 89 – Aviso de Instalação do Sistema Operacional

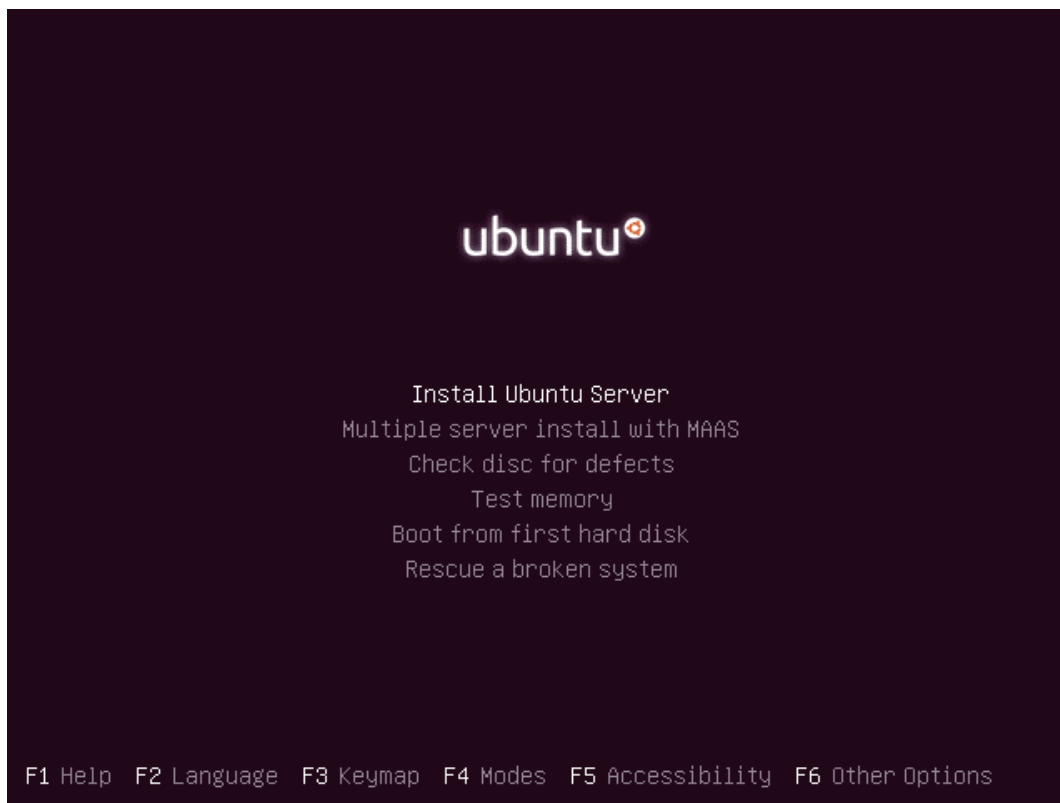


Figura 90 – Idioma para a Instalação

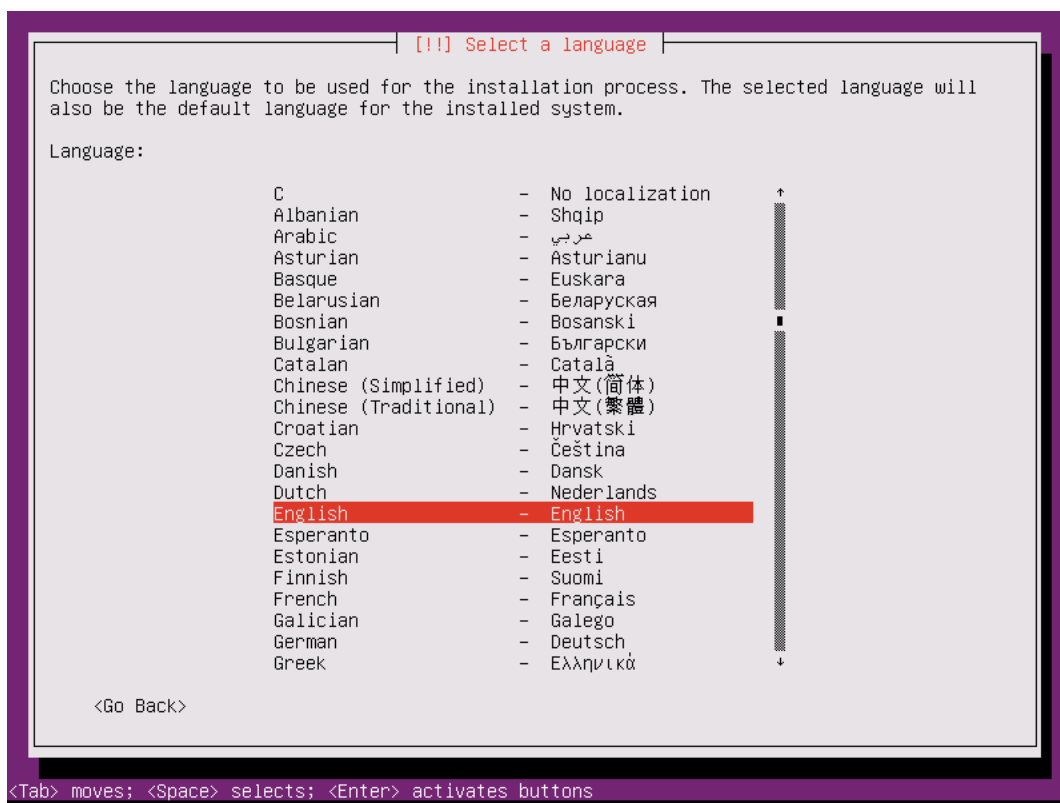


Figura 91 – Configuração de Localidade

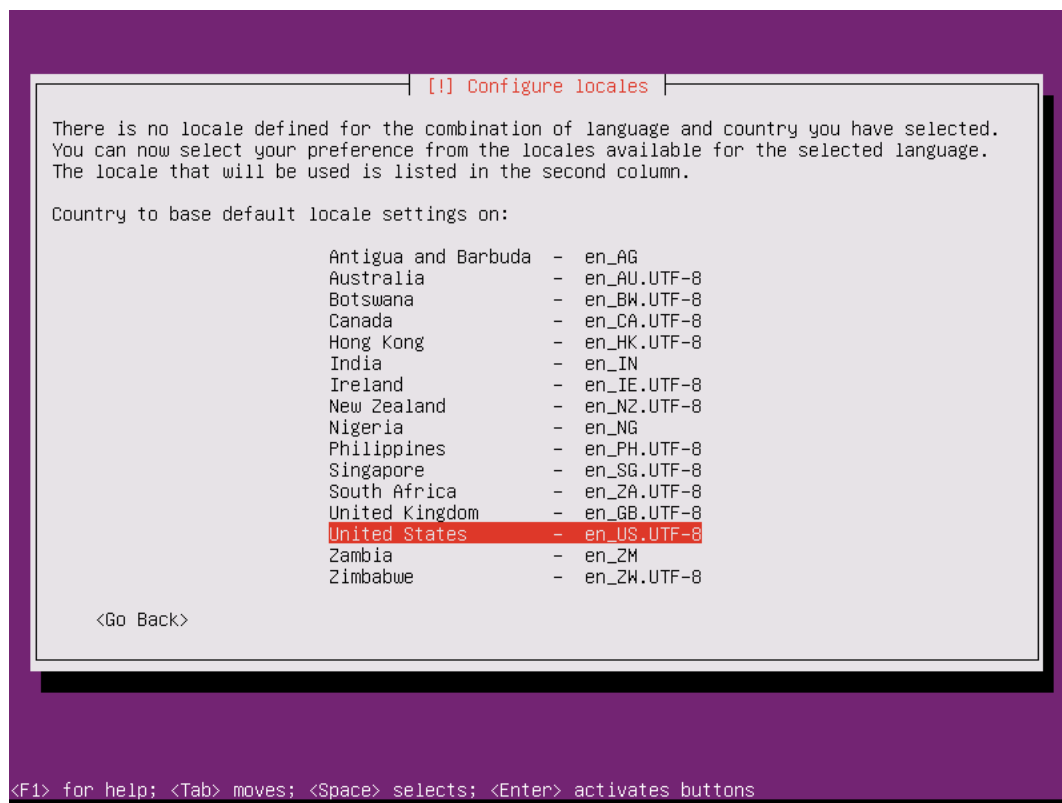


Figura 92 – Detecção de Teclado

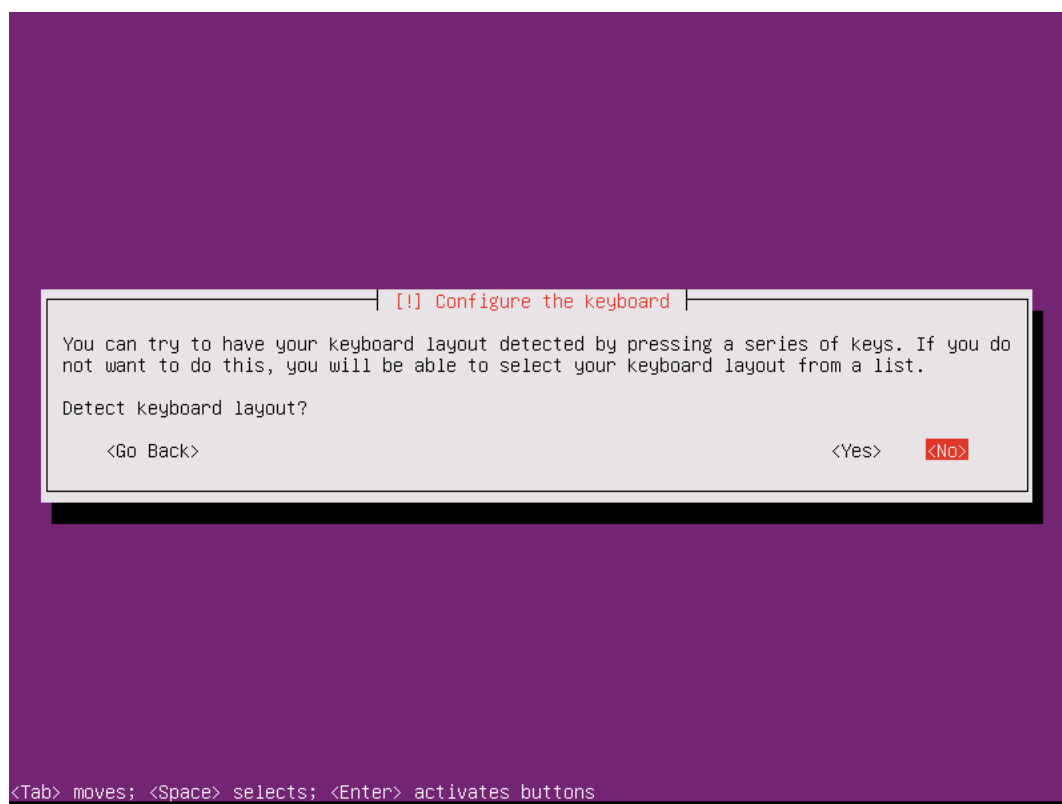
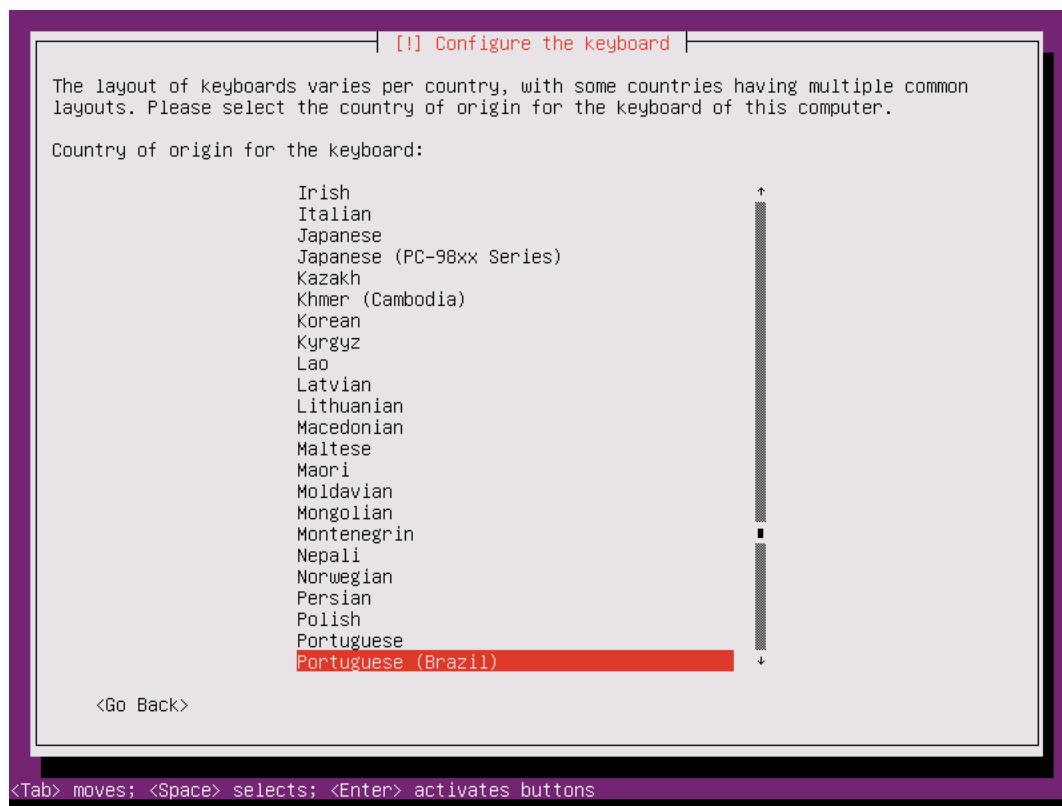


Figura 93 – Configuração de Idioma do Teclado



Uma das partes mais importantes da instalação é a criação do nome do servidor que deve ser escolhido com cuidado pois não poderá ser trocado quando o serviço de diretório estiver instalado e configurado.

Figura 94 – Nome do Servidor

[!] Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

ubuntu-server

<Go Back> <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons

Figura 95 – Usuário Administrador do Servidor

[!!] Set up users and passwords

A user account will be created for you to use instead of the root account for non-administrative activities.

Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user's real name. Your full name is a reasonable choice.

Full name for the new user:

administrator

<Go Back> <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons

Figura 96 – Usuário Administrador do Servidor

[!!] Set up users and passwords

Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters.

Username for your account:

administrator

<Go Back> <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons

Figura 97 – Senha do Usuário Administrador do Servidor

[!!] Set up users and passwords

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

Choose a password for the new user:

<Go Back> <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons

Figura 98 – Criptografar o Servidor

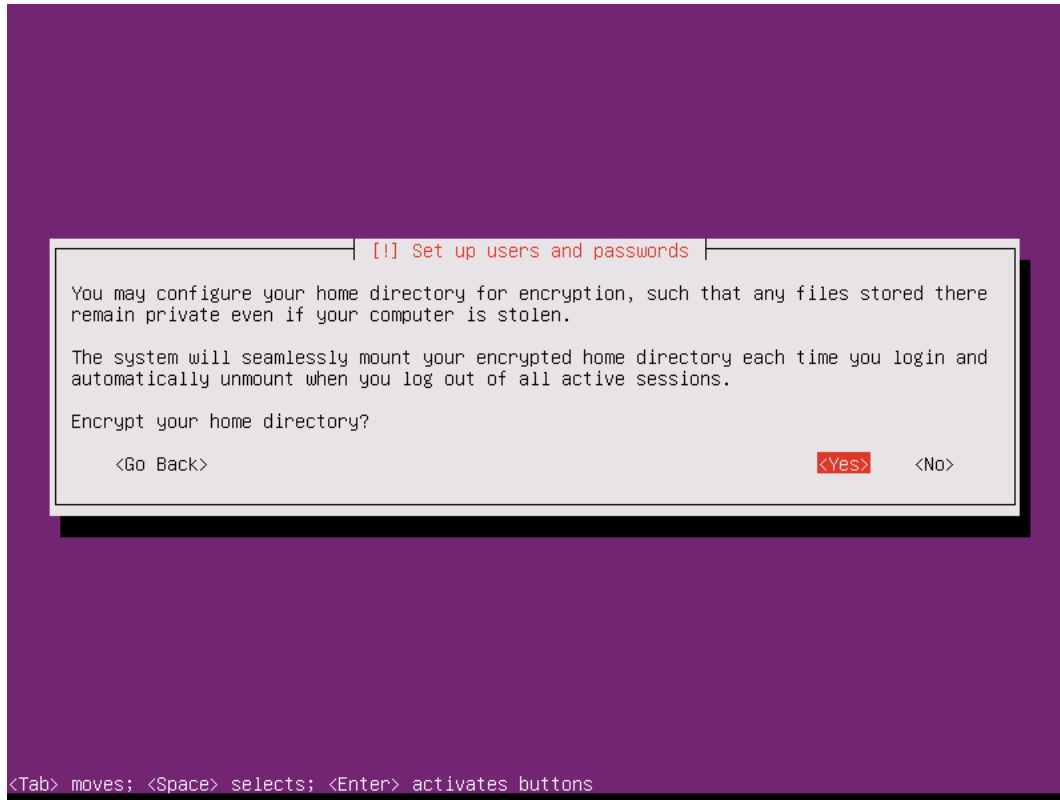
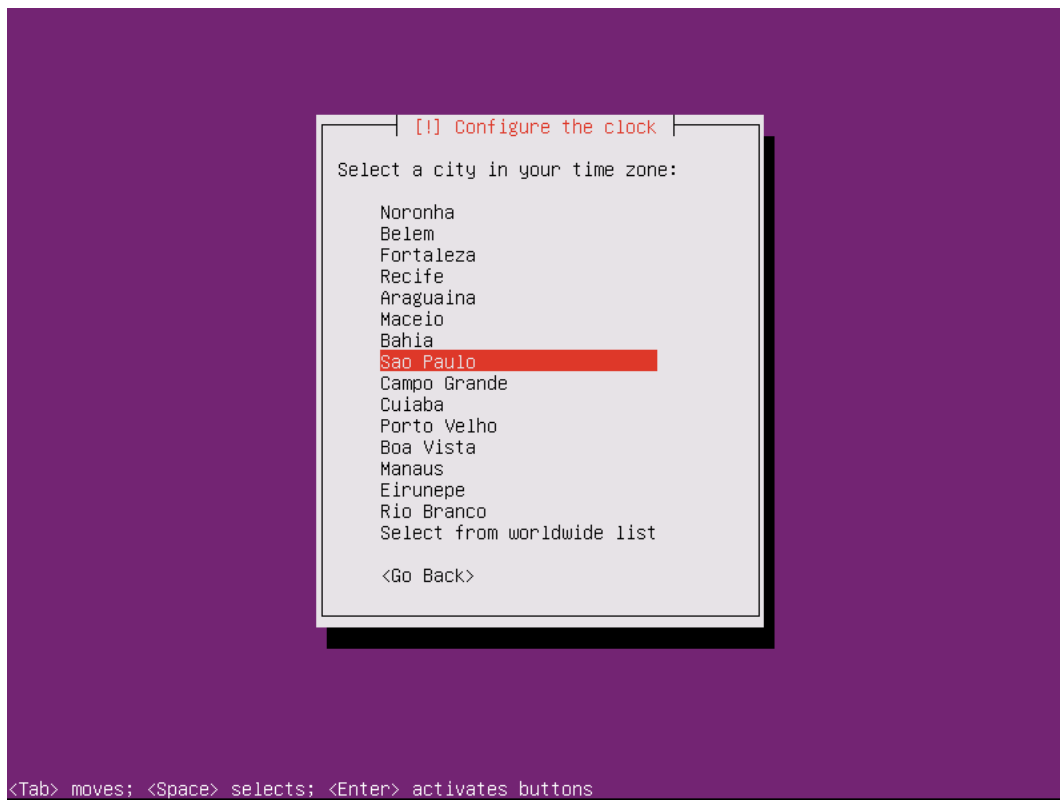


Figura 99 – Configuração de Horário do Servidor



Pela função do servidor ser inicialmente somente de controlador de domínio, o sistema será instalado em uma só partição com 16 Gb.

Figura 100 – Guia para Particionamento do Servidor

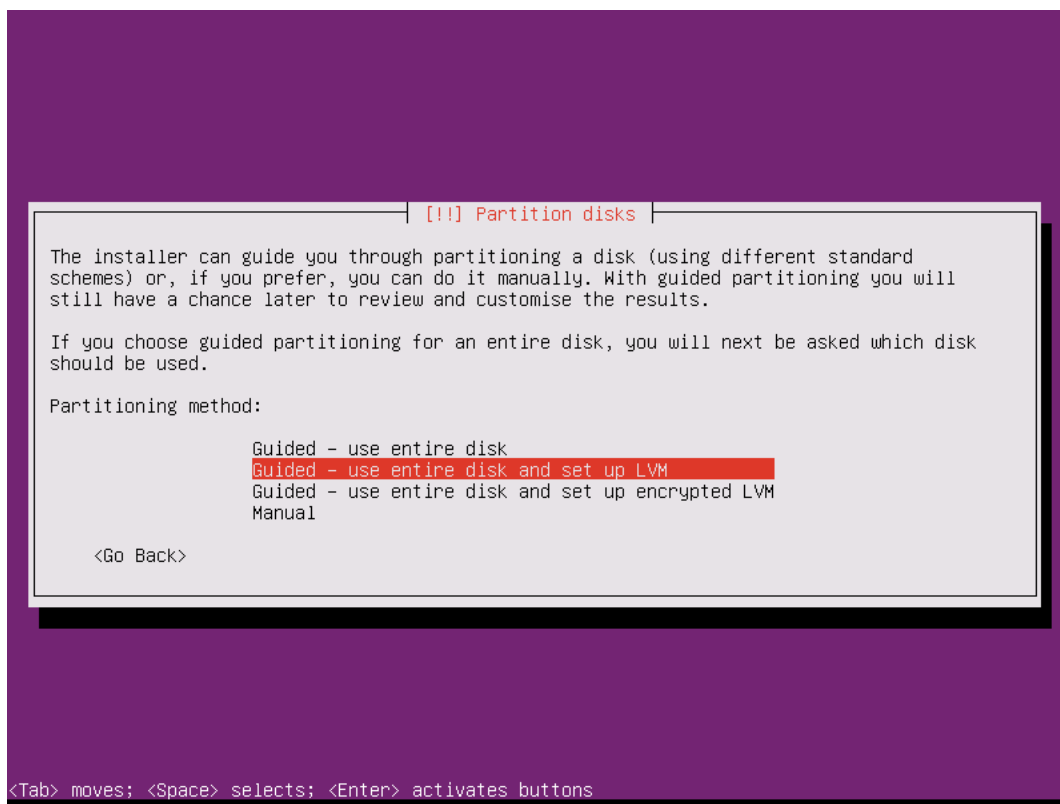


Figura 101 – Disco para Instalação

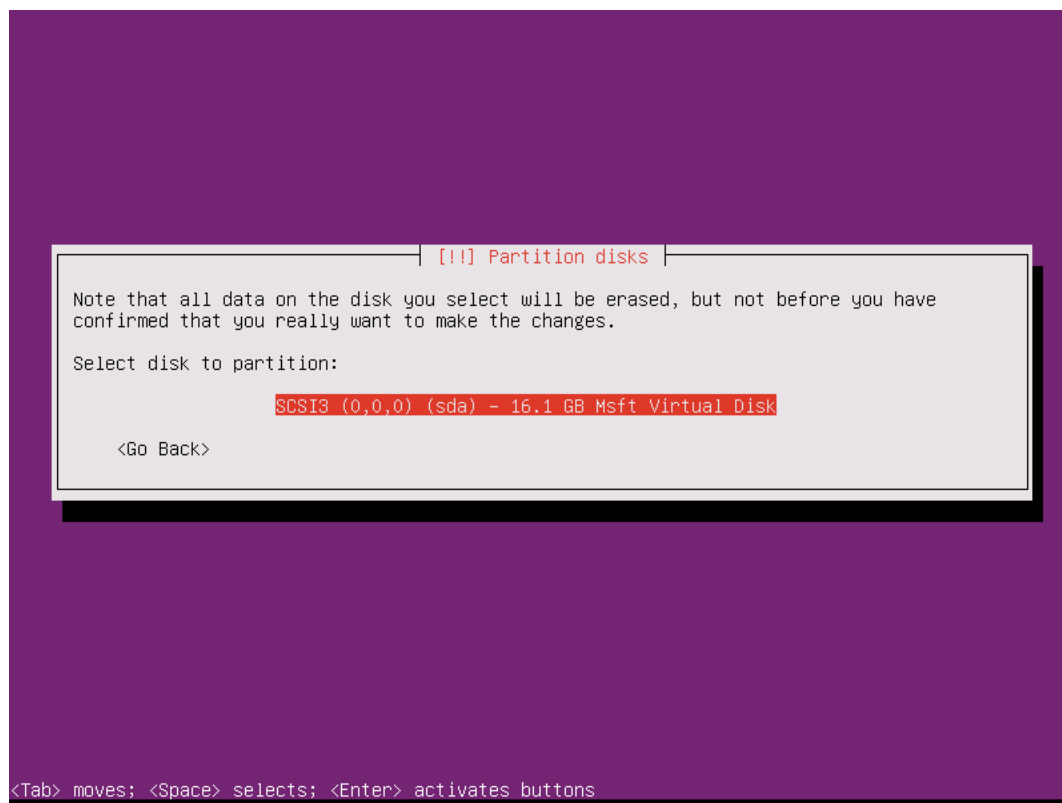


Figura 102 – Salvar Configurações

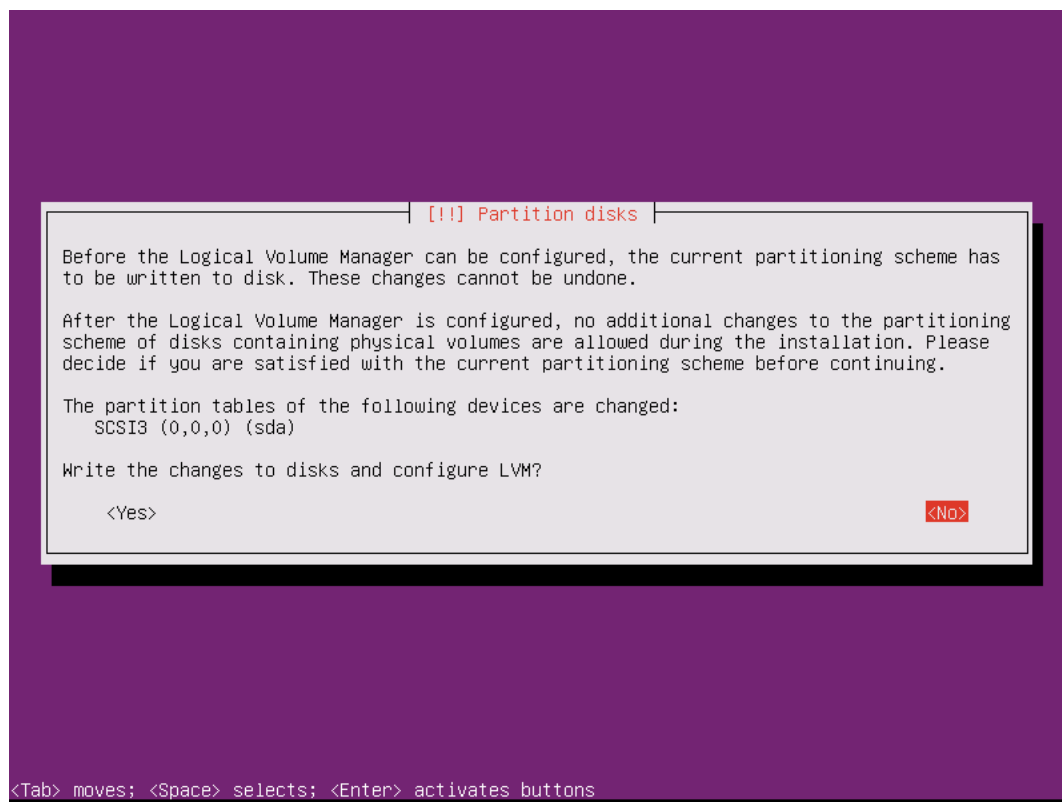


Figura 103 – Tamanho do Disco para Instalação

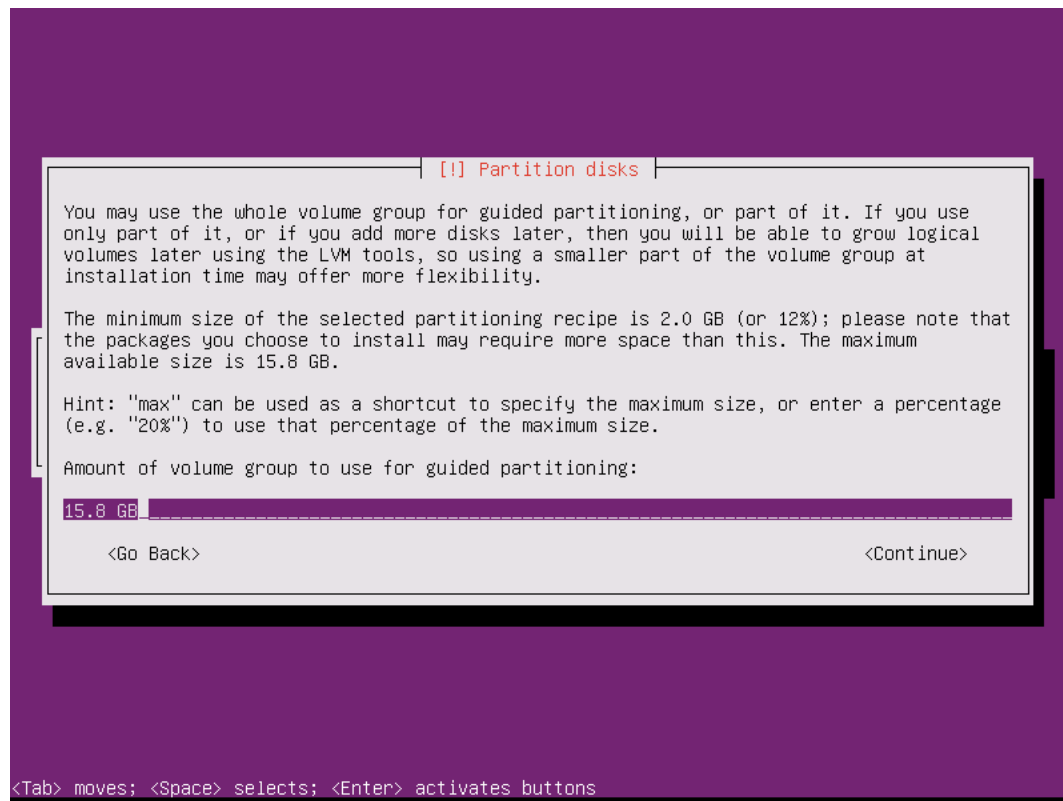
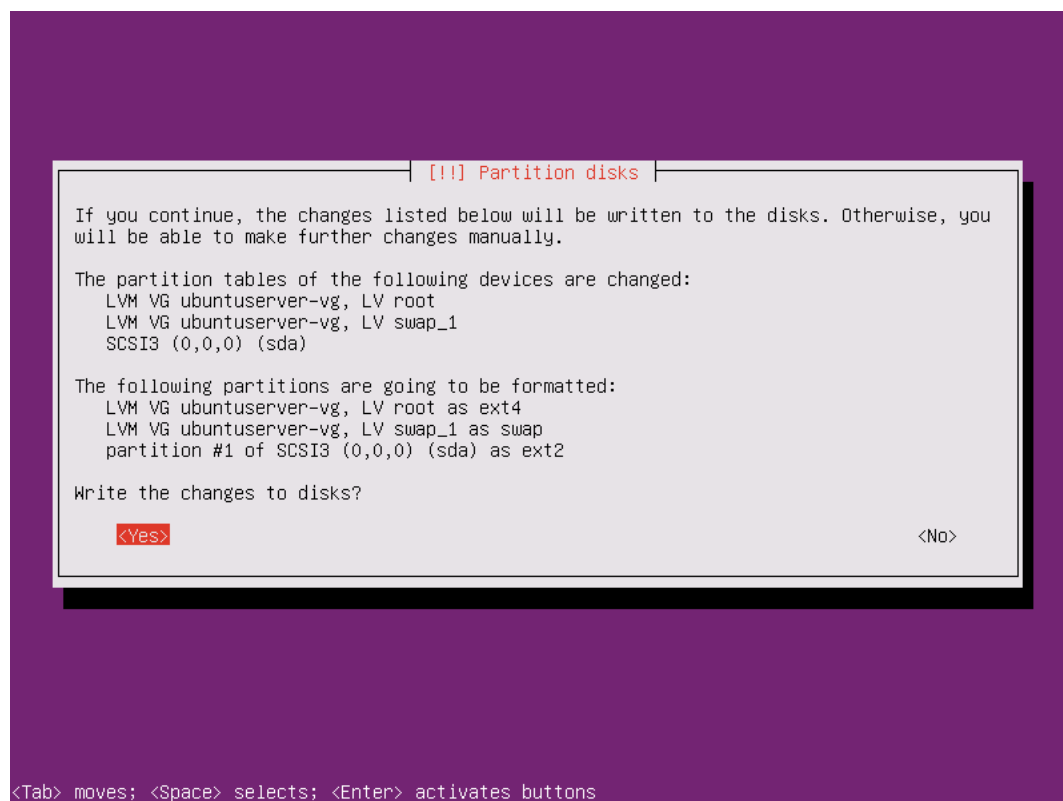
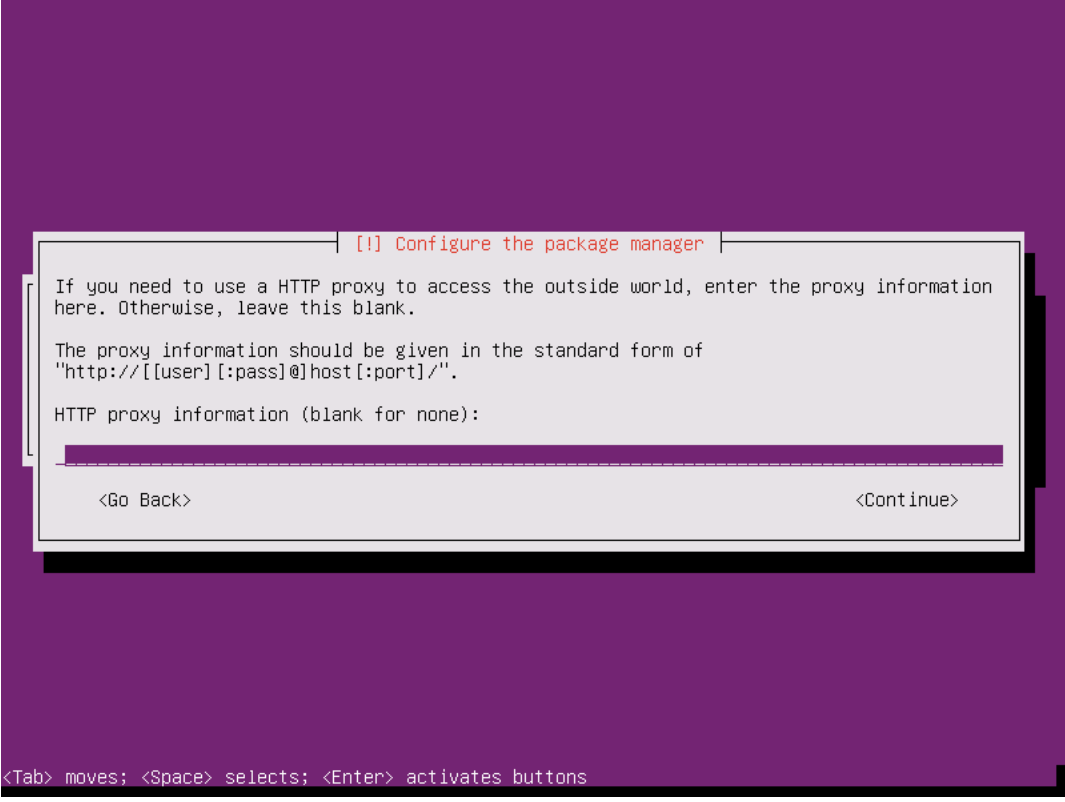


Figura 104 – Salvar Alterações no Disco



Como não existe proxy configurado esse questionamento é deixado em branco.

Figura 105 – Configuração de Proxy



The screenshot shows a terminal window with a purple background. A white box with a black border contains the following text:

[!] Configure the package manager

If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.

The proxy information should be given in the standard form of "http://[[user] [:pass]@]host[:port]/".

HTTP proxy information (blank for none):

Below the text is a long, empty input field with a dashed line underneath it.

At the bottom of the white box are two buttons: "<Go Back>" on the left and "<Continue>" on the right.

At the bottom of the terminal window, there is a line of text: "<Tab> moves; <Space> selects; <Enter> activates buttons".

Figura 106 – Instalar Atualizações Automaticamente

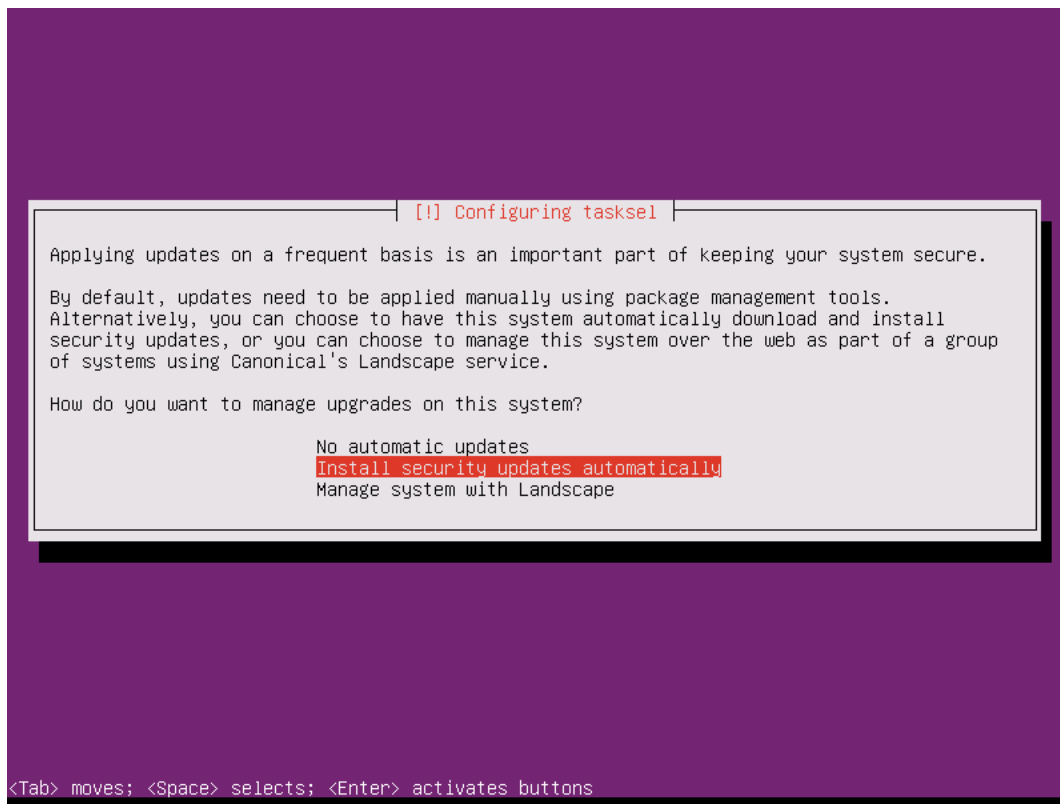


Figura 107 – Instalação da Aplicação SSH

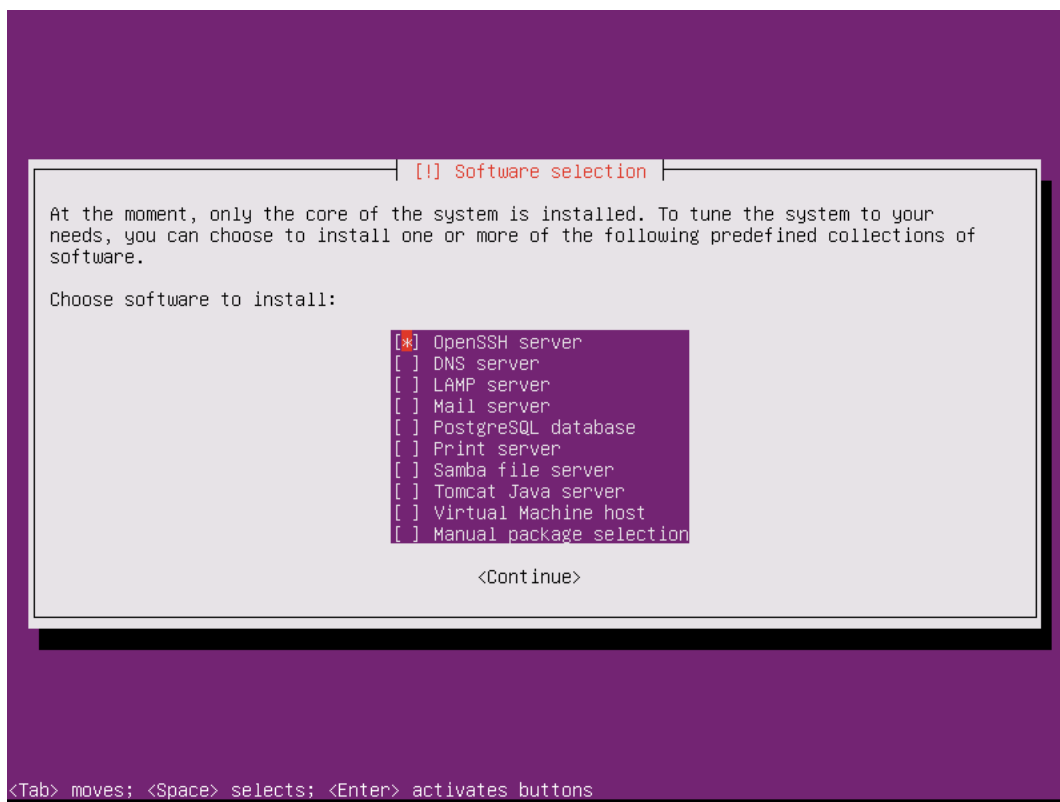
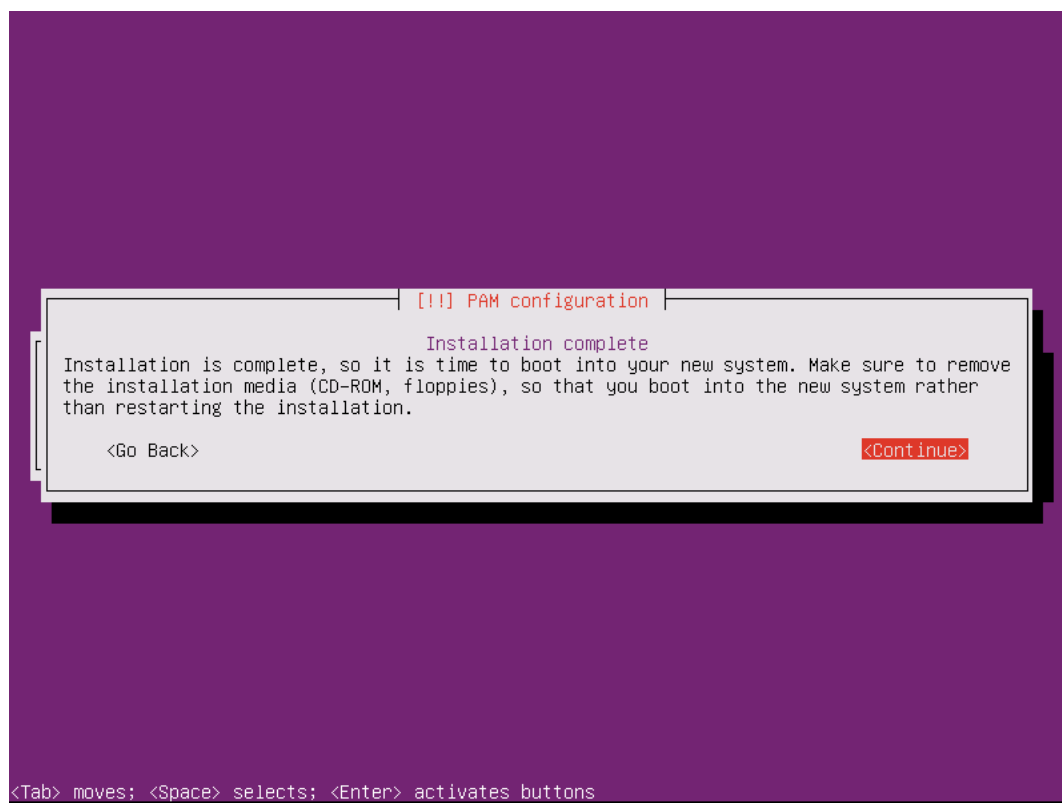


Figura 108 – Instalar o Carregador de Inicialização



Figura 109 – Instalação Completa



Após a instalação é preciso configurar o sistema.

5.2.3.2 Configuração do Controlador de Domínio

Inicialmente é preciso entrar com o usuário criado na instalação.

Figura 110 – Primeiro Acesso no Servidor



Em seguida configurar uma senha para usuário administrador.

Figura 111 – Configuração de Senha do Usuário

```

Ubuntu 14.04.1 LTS ubuntuuser tty1
ubuntuuser login: administrator
Password:
Login incorrect
ubuntuuser login: P@ssw0rd
Password:
Login incorrect
ubuntuuser login: administrator
Password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

System information as of Fri Sep 26 00:08:38 BRT 2014

System load:  1.53           Processes:      234
Usage of /:   8.0% of 13.37GB Users logged in:    0
Memory usage: 8%           IP address for eth0: 192.168.1.113
Swap usage:   0%

Graph this data and manage this system at:
https://landscape.canonical.com/

52 packages can be updated.
29 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

administrator@ubuntuuser:~$ _

```

Figura 112 – Confirmação de Senha do Usuário

```

Ubuntu 14.04.1 LTS ubuntuuser tty1
ubuntuuser login: administrator
Password:
Last login: Fri Sep 26 00:09:44 BRT 2014 on tty1
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

System information as of Fri Sep 26 01:03:32 BRT 2014

System load: 1.97           Memory usage: 7%   Processes:      222
Usage of /:  8.0% of 13.37GB Swap usage:   0%   Users logged in: 0

Graph this data and manage this system at:
https://landscape.canonical.com/

52 packages can be updated.
29 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

administrator@ubuntuuser:~$ sudo passwd root
[sudo] password for administrator:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
administrator@ubuntuuser:~$ _

```

5.2.3.3 Configurar IP Estático

Para estabelecer um servidor que tem um serviço estático na rede é preciso atribuir um IP estático ao servidor. Para essa configuração foi usado o IP 192.168.1.100 classe C. Para fazer essa configuração é preciso modificar as configurações no diretório de redes do servidor usando o seguinte comando: `vi /etc/network/interfaces`. Com esse comando é possível editar as configurações da placa de rede.

Figura 113 – Verificação de IP

```
root@ubuntu:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:15:5d:ea:c0:35
          inet addr:192.168.1.113  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::215:5dff:feac035/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3710 errors:0 dropped:0 overruns:0 frame:0
          TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1187826 (1.1 MB)  TX bytes:10964 (10.9 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1184 (1.1 KB)  TX bytes:1184 (1.1 KB)

root@ubuntu:~# vi /etc/network/interfaces
```

Figura 114 – Configuração da Interface

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp

"/etc/network/interfaces" 10L, 268C 1,1 All
```

Figura 115 – Configuração da Interface com Valores Estáticos

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static

address 192.168.1.100
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
dns-nameservers 192.168.1.100 8.8.8.8
dns-search monografia.local

-- INSERT -- 18,28 All
```


5.2.3.4 Modificar o Nome do Computador

Para modificar o nome do computador é preciso editar o arquivo que contem o nome do computador com o comando: `vi /etc/hosts`. Assim completar o nome do host com nome dele no formato do futuro domínio que será MONOGRAFIA.LOCAL e o seu novo IP atribuído estaticamente.

Figura 116 – Acessando o Arquivo de Hosts

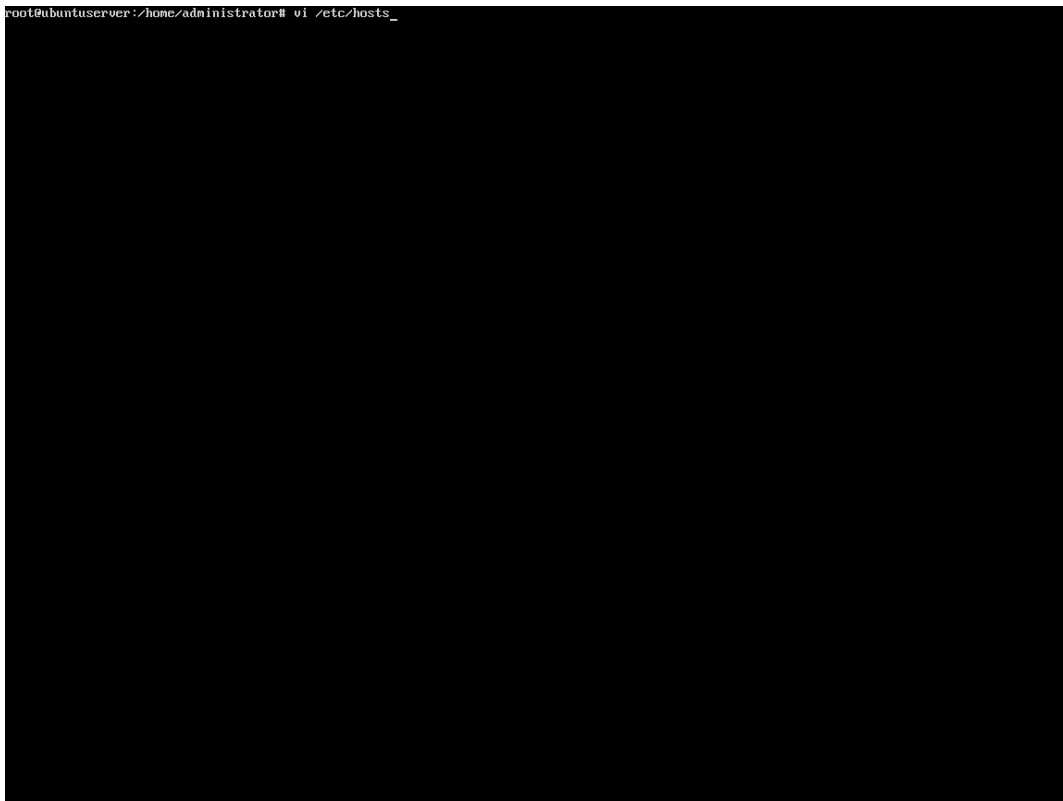



Figura 117 – Configurando o Arquivo de Hosts

```
127.0.0.1      localhost
127.0.1.1      ubuntu:server

# The following lines are desirable for IPv6 capable hosts
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
```

Figura 119 – Salvando a Configuração no Hosts



```
root@ubuntuserver:/home/administrator# echo ubuntuserver.monografia.local > /etc/hostname
root@ubuntuserver:/home/administrator# _
```

5.2.3.5 Atualizar o Sistema

Para fazer a instalação do SAMBA é preciso fazer a atualização completa do sistema, para isso é preciso rodar os comandos *apt-get update* e *apt-get upgrade*.

Figura 120 – Upgrade do Ubuntu Server



```
administrator@ubuntu-server:~$ su
Password:
root@ubuntu-server:/home/administrator# apt-get update && apt-get upgrade -y
```

5.2.3.6 Pré-requisitos

Para que o SAMBA funcione como planejado é preciso instalar pacotes que são pré-requisitos para fazer o SAMBA se tornar um controlador de domínio, como o pacote *krb5-user* que fornece suporte a autenticação kerberos do Windows. Para isso é preciso instalar os pacotes com o seguinte comando: *apt-get install git build-essential libacl1-dev libattr1-dev libblkid-dev libgnutls-dev libreadline-dev python-dev python-dnspython gdb pkg-config libpopt-dev libldap2-dev dnsutils libbsd-dev attr krb5-user docbook-xsl libcups2-dev libpam0g-dev ntp -y*.

Uma vez instalado, o pacote *krb5-user* questiona qual será o nome do futuro domínio e o nome do servidor que terá o domínio, no caso o nome do domínio escolhido foi MONOGRAFIA.LOCAL e o nome do servidor *ubuntu-server*.

Figura 121 – Instalação do Kerberos



Figura 122 – Inclusão de Nome do Domínio

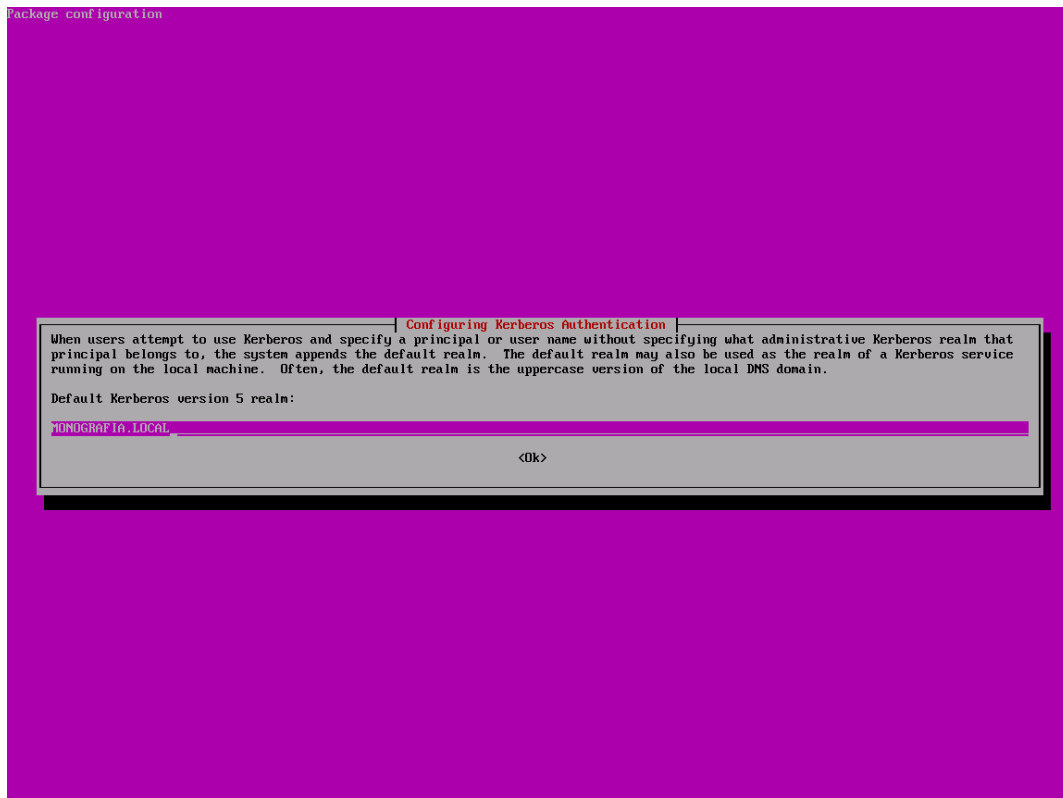


Figura 123 – Inclusão do Nome do Servidor Kerberos

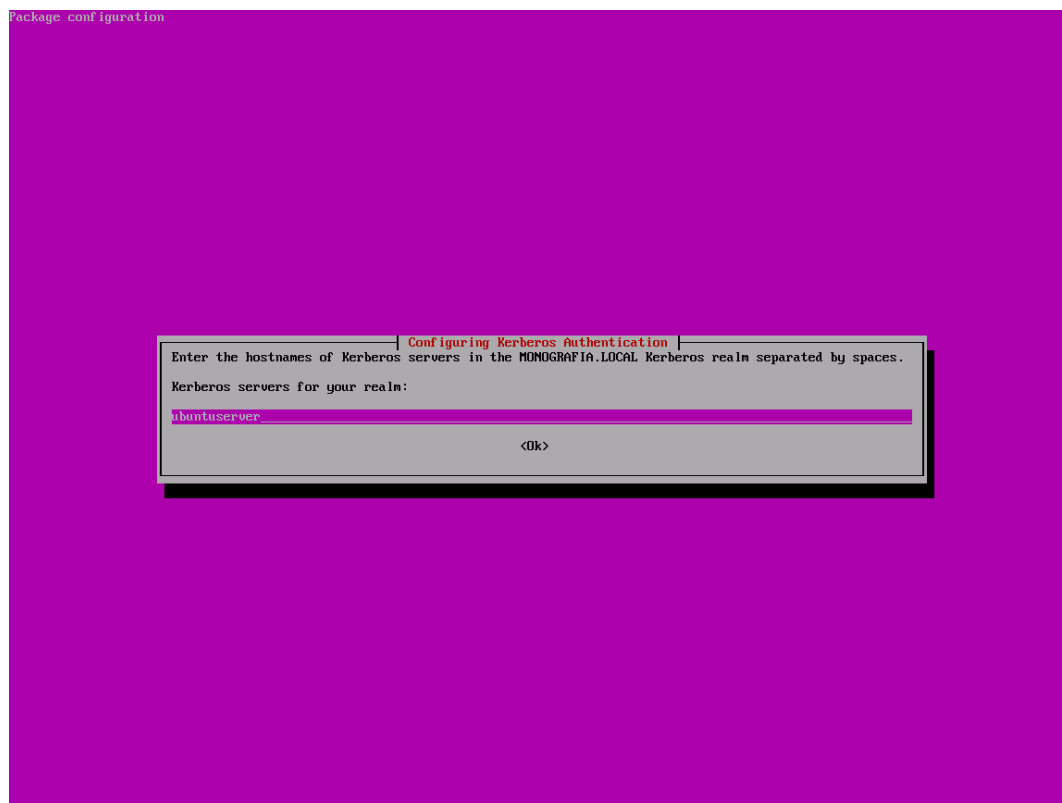
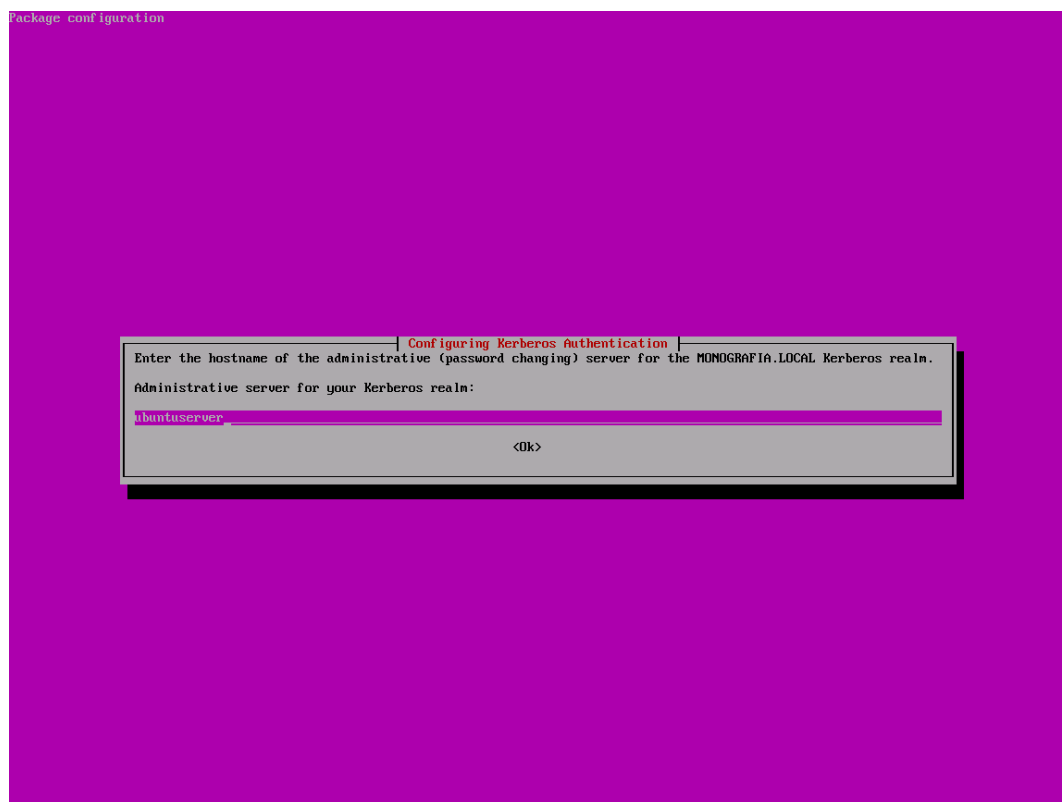


Figura 124 – Inclusão do Nome do Servidor de Administração

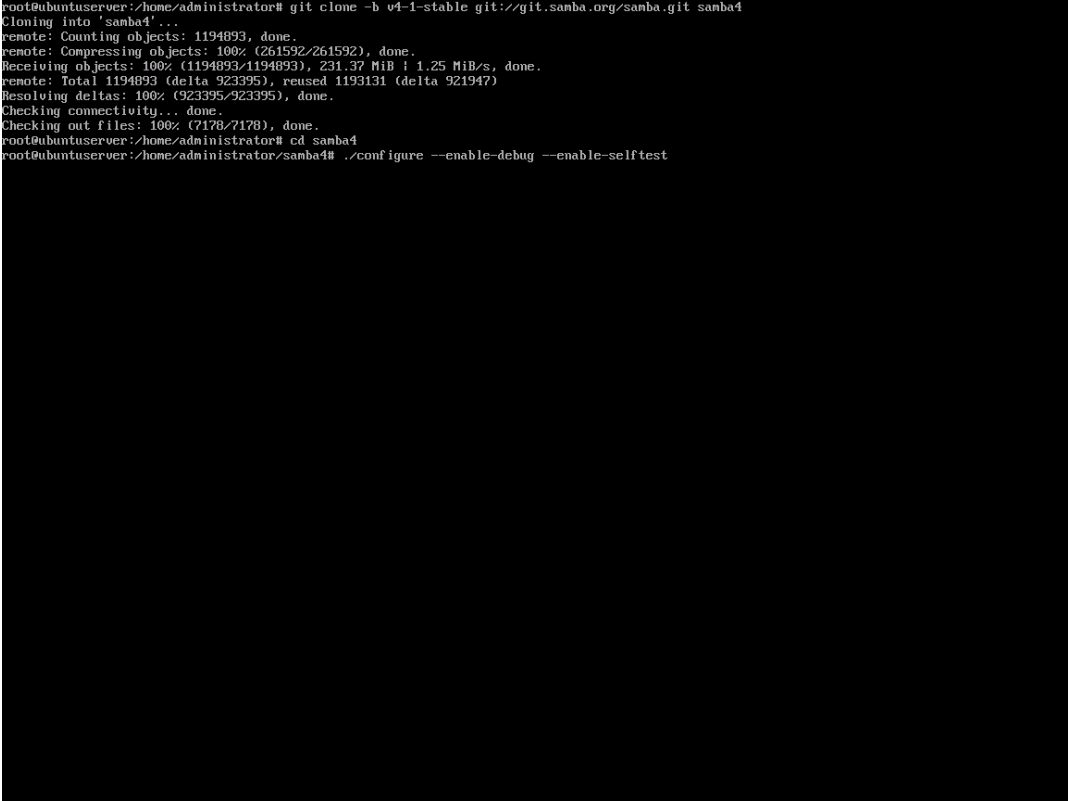


5.2.3.7 Instalação do SAMBA

Para fazer a instalação do SAMBA é preciso fazer uma cópia do programa de uma página de downloads na internet e depois compilar o programa. De acordo com os tutoriais o SAMBA 4 precisa ser copilado pois ainda não existia no repositório do comando apt-get. O comando usado para baixar o SAMBA 4 é: *git clone -b v4-0-stable git://git.samba.org/samba.git samba4*. Uma vez baixado o programa é preciso ir até a pasta do programa e executar a seguinte sequencia de comandos para compila-lo:

- *./configure --enable-debug --enable-selftest*
- *make*
- *make install*

Figura 125 – Comando Debug do Clone



```
root@ubuntu-server:/home/administrator# git clone -b v4-1-stable git://git.samba.org/samba.git samba4
Cloning into 'samba4' ...
remote: Counting objects: 1194893, done.
remote: Compressing objects: 100% (261592/261592), done.
Receiving objects: 100% (1194893/1194893), 231.37 MiB | 1.25 MiB/s, done.
remote: Total 1194893 (delta 923395), reused 1193131 (delta 921947)
Resolving deltas: 100% (923395/923395), done.
Checking connectivity... done.
Checking out files: 100% (7178/7178), done.
root@ubuntu-server:/home/administrator# cd samba4
root@ubuntu-server:/home/administrator/samba4# ./configure --enable-debug --enable-selftest
```

Figura 126 – Comando Make

```

getcwd takes a NULL argument : ok
Checking for library gen : not found
Checking for getsipman : ok
Checking for header sys/fs/vx_quota.h : no
Checking for header sys/quota.h : yes
Checking for header ufs/ufs/quota.h : no
Checking for header xfs/xqm.h : no
for XFS QUOTA in <sys/quota.h> : not found
Checking for member dqbfsoftlimit in struct dqblk : not found
Checking for member dqbfcurbytes in struct dqblk : not found
Checking for header rpcsvc/rquota.h : yes
Checking for member getquota_rslt_u in struct getquota_rslt : ok
Checking for header ctdb.h : not found
building without cluster support: ctdb.h is required for cluster support
Checking whether we can compile with __attribute__((destructor)) : ok
Checking whether seekdir returns void : ok
Checking for pthread_attr_t : ok
Checking for header gpf.h : no
Checking for header linux/ioctl.h : yes
Checking for header cephfs/libcephfs.h : no
Checking for glusterfs-api >= 4 : not found
Checking for header api/glfs.h : no
Checking for library gapi : no
looking for ncurses features
Checking for program ncurses5-config : /usr/bin/ncurses5-config
Checking for header ncurses5-config : yes
Checking for header menu.h : no
Checking for header panel.h : no
Checking for header form.h : no
Checking for library ncurses : not found
Checking for initscr : not found
Checking for library menu : not found
Checking for set_menu_items : not found
Checking for item_count : not found
Checking for library panel : not found
Checking for new_panel : not found
Checking for show_panel : not found
Checking for library form : not found
Checking for new_field : not found
Checking for new_form : not found
ncurses not available, not building regedit
Checking linker accepts -Wl,-no-undefined : yes
Checking linker accepts ['undefined', 'dynamic_lookup'] : no
Checking linker accepts -Wl,--as-needed : yes
Checking for -lc not needed : ok
Checking configure summary : ok
Checking compiler for PIE support : yes
Checking for libsystemd-daemon : not found
Checking for header systemd/sd-daemon.h : no
Checking for library systemd-daemon : no
Checking compiler accepts -g : yes
configure finished successfully (3m22.907s)
root@ubuntu-server:/home/administrator/samba4# make

```

Figura 127 – Comando Make Install

```

[3796/3842] Linking default/source3/modules/libofs-aiio-fork.so
[3797/3842] Linking default/source3/modules/libofs-default-quota.so
[3798/3842] Linking default/source3/pysmbd.so
[3799/3842] Linking default/source3/modules/libofs-fake-perms.so
[3800/3842] Linking default/source3/modules/libofs-readonly.so
[3801/3842] Linking default/source3/modules/libofs-smb-traffic-analyzer.so
[3802/3842] Linking default/source3/modules/libofs-dirsort.so
[3803/3842] Linking default/source3/modules/libofs-aiio-posix.so
[3804/3842] Linking default/source3/modules/libofs-nfsacl-xattr.so
[3805/3842] Linking default/source3/modules/libofs-acl-xattr.so
[3806/3842] Linking default/source3/modules/libofs-xattr-tdb.so
[3807/3842] Linking default/source3/modules/libofs-shadow-copy.so
[3808/3842] Linking default/source3/modules/libofs-netatalk.so
[3809/3842] Linking default/source3/modules/libofs-full-audit.so
[3810/3842] Linking default/source3/modules/libofs-catia.so
[3811/3842] Linking default/source3/modules/libofs-recycle.so
[3812/3842] Linking default/source3/modules/libofs-aiio-pthread.so
[3813/3842] Linking default/source3/modules/libofs-fake-acls.so
[3814/3842] Linking default/source3/modules/libofs-streams-xattr.so
[3815/3842] Linking default/source3/modules/libofs-extd-audit.so
[3816/3842] Linking default/source3/modules/libofs-cap.so
[3817/3842] Linking default/source3/modules/libofs-linux-xfs-sgid.so
[3818/3842] Linking default/source3/smbd/smbd
[3819/3842] Linking default/source3/ufstest
[3820/3842] Linking default/source3/modules/libofs-streams-depot.so
[3821/3842] Linking default/source3/modules/libofs-scannedonly.so
[3822/3842] Linking default/source3/modules/libofs-posix-eadb.so
[3823/3842] Linking default/source3/modules/libofs-btrfs.so
[3824/3842] Linking default/source3/modules/libofs-audit.so
[3825/3842] Linking default/source3/modules/libnon_posix_acls.so
[3826/3842] Linking default/source3/smbstatus
[3827/3842] Linking default/source3/modules/libofs-syncops.so
[3828/3842] Linking default/source3/modules/libofs-readahead.so
[3829/3842] Linking default/source3/modules/libofs-net
[3830/3842] Linking default/source3/net
[3831/3842] Linking default/source3/modules/libofs-expand-mdfs.so
[3832/3842] Linking default/source3/modules/libofs-shadow-copy2.so
[3833/3842] Linking default/source3/modules/libofs-crossrename.so
[3834/3842] Linking default/source3/modules/libofs-acl-tdb.so
[3835/3842] Linking default/source3/modules/libofs-preopen.so
[3836/3842] Linking default/source3/modules/libofs-media-harmony.so
[3837/3842] pid1: pid1 -> bin/default/pid1/pid1
[3838/3842] Parse::Pid1::Dump:3pm: pid1/lib/Parse/Pid1/Dump.pm -> bin/default/pid1/Parse::Pid1::Dump:3pm
[3839/3842] Parse::Pid1::Wireshark::Conformance:3pm: pid1/lib/Parse/Pid1/Wireshark/Conformance.pm -> bin/default/pid1/Parse::Pid1::Wireshark::Co
nformance:3pm
[3840/3842] Parse::Pid1::Util:3pm: pid1/lib/Parse/Pid1/Util.pm -> bin/default/pid1/Parse::Pid1::Util:3pm
[3841/3842] Parse::Pid1::NDR:3pm: pid1/lib/Parse/Pid1/NDR.pm -> bin/default/pid1/Parse::Pid1::NDR:3pm
[3842/3842] Parse::Pid1::Wireshark::NDR:3pm: pid1/lib/Parse/Pid1/Wireshark/NDR.pm -> bin/default/pid1/Parse::Pid1::Wireshark::NDR:3pm
inf: leaving directory /home/administrator/samba4/bin
[build] finished successfully (40m35.860s)
root@ubuntu-server:/home/administrator/samba4#
root@ubuntu-server:/home/administrator/samba4#
root@ubuntu-server:/home/administrator/samba4#
root@ubuntu-server:/home/administrator/samba4# make install

```


5.2.3.8 Criação do Domínio

Para fazer a instalação do domínio é preciso ir ao arquivo de configuração do SAMBA o *samba-tool*. Para isso foi usado o seguinte comando: */usr/local/samba/bin/samba-tool domain provision --realm=monografia.local --domain=MONOGRAFIA --adminpass="P@ssw0rd" --server-role=dc --dns-backend=SAMBA_INTERNAL*.

Uma vez que o domínio está configurado é preciso iniciar o serviço do SAMBA usando o comando */usr/local/samba/sbin/samba*.

Figura 128 – Criação do Domínio

```

with_with.py
* installing lib/testtools/testtools/testsuite.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/testtools/testsuite.py
* installing lib/testtools/testtools/utils.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/testtools/utils.py
* installing lib/subunit/python/subunit/_init_.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/_init_.py
* installing lib/subunit/python/subunit/chunked.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/chunked.py
* installing lib/subunit/python/subunit/details.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/details.py
* installing lib/subunit/python/subunit/filters.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/filters.py
* installing lib/subunit/python/subunit/isob601.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/isob601.py
* installing lib/subunit/python/subunit/progress_model.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/progress_model.py
py
* installing lib/subunit/python/subunit/run.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/run.py
* installing lib/subunit/python/subunit/test_results.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/test_results.py
* installing lib/subunit/python/subunit/tests/TestUtil.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/tests/TestUtil.py
py
* installing lib/subunit/python/subunit/tests/_init_.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/tests/_init_.py
* installing lib/subunit/python/subunit/tests/sample-script.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/tests/sample-script.py
* installing lib/subunit/python/subunit/tests/sample-two-script.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/tests/sample-two-script.py
* installing lib/subunit/python/subunit/tests/test_chunked.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/tests/test_chunked.py
* installing lib/subunit/python/subunit/tests/test_details.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/tests/test_details.py
* installing lib/subunit/python/subunit/tests/test_progress_model.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/tests/test_progress_model.py
* installing lib/subunit/python/subunit/tests/test_run.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/tests/test_run.py
py
* installing lib/subunit/python/subunit/tests/test_subunit_filter.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/tests/test_subunit_filter.py
* installing lib/subunit/python/subunit/tests/test_subunit_stats.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/tests/test_subunit_stats.py
* installing lib/subunit/python/subunit/tests/test_subunit_tags.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/tests/test_subunit_tags.py
* installing lib/subunit/python/subunit/tests/test_tap2subunit.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/tests/test_tap2subunit.py
* installing lib/subunit/python/subunit/tests/test_test_protocol.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/tests/test_test_protocol.py
* installing lib/subunit/python/subunit/tests/test_test_results.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/tests/test_test_results.py
* installing bin/default/pidl/pidl.1p as /usr/local/samba/share/man/man1/pidl.1p
* installing bin/default/pidl/Parse::Pidl::Dump.3pm as /usr/local/samba/share/man/man3/Parse::Pidl::Dump.3pm
* installing bin/default/pidl/Parse::Pidl::Wireshark::Conformance.3pm as /usr/local/samba/share/man/man3/Parse::Pidl::Wireshark::Conformance.3pm
* installing bin/default/pidl/Parse::Pidl::Util.3pm as /usr/local/samba/share/man/man3/Parse::Pidl::Util.3pm
* installing bin/default/pidl/Parse::Pidl::NDR.3pm as /usr/local/samba/share/man/man3/Parse::Pidl::NDR.3pm
* installing bin/default/pidl/Parse::Pidl::Wireshark::NDR.3pm as /usr/local/samba/share/man/man3/Parse::Pidl::Wireshark::NDR.3pm
saf: Leaving directory /home/administrator/samba4/bin
saf: install finished successfully (46s3.136s)
root@santuserver:/home/administrator/samba4#
root@santuserver:/home/administrator/samba4#
root@santuserver:/home/administrator/samba4#
root@santuserver:/home/administrator/samba4#
root@santuserver:/home/administrator/samba4# /usr/local/samba/bin/samba-tool domain provision --realm=monografia.local --domain=MONOGRAFIA --adminpass="P@ssw0rd" --server-role=dc --dns-backend=SAMBA_INTERNAL

```

Figura 129 – Iniciar Serviço do SMB

```

* installing bin/default/pidl/Parse::Pidl::Dump.3pm as /usr/local/samba/share/man/man3/Parse::Pidl::Dump.3pm
* installing bin/default/pidl/Parse::Pidl::Wireshark::Conformance.3pm as /usr/local/samba/share/man/man3/Parse::Pidl::Wireshark::Conformance.3pm
* installing bin/default/pidl/Parse::Pidl::Util.3pm as /usr/local/samba/share/man/man3/Parse::Pidl::Util.3pm
* installing bin/default/pidl/Parse::Pidl::NDR.3pm as /usr/local/samba/share/man/man3/Parse::Pidl::NDR.3pm
* installing bin/default/pidl/Parse::Pidl::Wireshark::NDR.3pm as /usr/local/samba/share/man/man3/Parse::Pidl::Wireshark::NDR.3pm
saf: Leaving directory '/home/administrator/samba4/bin'
'install' finished successfully (16m3.136s)
root@ubuntu:~/home/administrator/samba4#
root@ubuntu:~/home/administrator/samba4#
root@ubuntu:~/home/administrator/samba4#
root@ubuntu:~/home/administrator/samba4# /usr/local/samba/bin/samba-tool domain provision --realm=monografia.local --domain=MONOGRAFIA --ad
minpass="P@ssw0rd" --server-role=dc --dns-backend=SAMBA_INTERNAL
Looking up IPv4 addresses
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=monografia,DC=local
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=monografia,DC=local
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba 4 has been generated at /usr/local/samba/private/krb5.conf
Once the above files are installed, your Samba4 server will be ready to use
Server Role: active directory domain controller
Hostname: ubuntu
NetBIOS Name: MONOGRAFIA
DNS Domain: monografia.local
DOMAIN SID: S-1-5-21-3695693990-2571106505-2963212893
root@ubuntu:~/home/administrator/samba4#
root@ubuntu:~/home/administrator/samba4# /usr/local/samba/sbin/samba

```

5.2.3.9 Configuração do DNS

Para configurar o DNS no domínio é preciso incluir o domínio no arquivo *resolv.conf* e editar o arquivo de configuração do SAMBA, o *smb.conf*. Para modificar o arquivo de configuração é preciso usar o comando: *vi /usr/local/etc/smb.conf*. Ao editar o arquivo é preciso substituir o *forwarder* para o IP do Google, 8.8.8.8, salvar e fechar o arquivo.

Figura 130 – Comando Configuração do DNS

```

root@ubuntu-server:/home/administrator/samba4# /usr/local/samba/sbin/samba -U
Version 4.1.12
root@ubuntu-server:/home/administrator/samba4# /usr/local/samba/bin/smbclient -U
Version 4.1.12
root@ubuntu-server:/home/administrator/samba4# /usr/local/samba/bin/smbclient -L localhost -Uz
Domain=[MONOGRAFIA] OS=[Unix] Server=[Samba 4.1.12]

      Sharename      Type            Comment
      -----
netlogon             Disk
sysvol               Disk
IPC$                 IPC           IPC Service (Samba 4.1.12)
Domain=[MONOGRAFIA] OS=[Unix] Server=[Samba 4.1.12]

      Server            Comment
      -----
Workgroup              Master

root@ubuntu-server:/home/administrator/samba4# echo domain MONOGRAFIA.LOCAL >> /etc/resolv.conf
root@ubuntu-server:/home/administrator/samba4# vi /usr/local/samba/etc/smb.conf_

```

Figura 131 – Arquivo de Configuração do DNS

```

# Global parameters
[global]
    workgroup = MONOGRAFIA
    realm = monografia.local
    netbios name = UBUNTUSERVER
    server role = active directory domain controller
    dns forwarder = 192.168.1.100

[netlogon]
    path = /usr/local/samba/var/locks/sysvol/monografia.local/scripts
    read only = No

[sysvol]
    path = /usr/local/samba/var/locks/sysvol
    read only = No

```

Figura 132 – Arquivo de Configuração do DNS com IP do Google

```
# Global parameters
[global]
    workgroup = MONOGRAFIA
    realm = monografia.local
    netbios name = UBUNTUSERVER
    server role = active directory domain controller
    dns forwarder = 8.8.8.8

[netlogon]
    path = /usr/local/samba/var/locks/sysvol/monografia.local/scripts
    read only = No

[sysvol]
    path = /usr/local/samba/var/locks/sysvol
    read only = No
```

-- INSERT --

7,25-32 011

5.2.3.10 Configurar o Kerberos

Para configurar o *Kerberos* no Linux é preciso editar o arquivo de configuração *krb5.conf* entrando com o comando: *vi /usr/local/samba/share/setup/krb5.conf*. Ao entrar no arquivo de configuração é preciso substituir a expressão *\$(REALM)* por *MONOGRAFIA.LOCAL* e em seguida realizar um teste para verificar o funcionamento. Para realizar o teste é preciso usar a seguinte sequência de comandos: *kinit administrator@MONOGRAFIA.LOCAL* e *klist -e*.

Figura 133 –Comando para Configurar o Kerberos

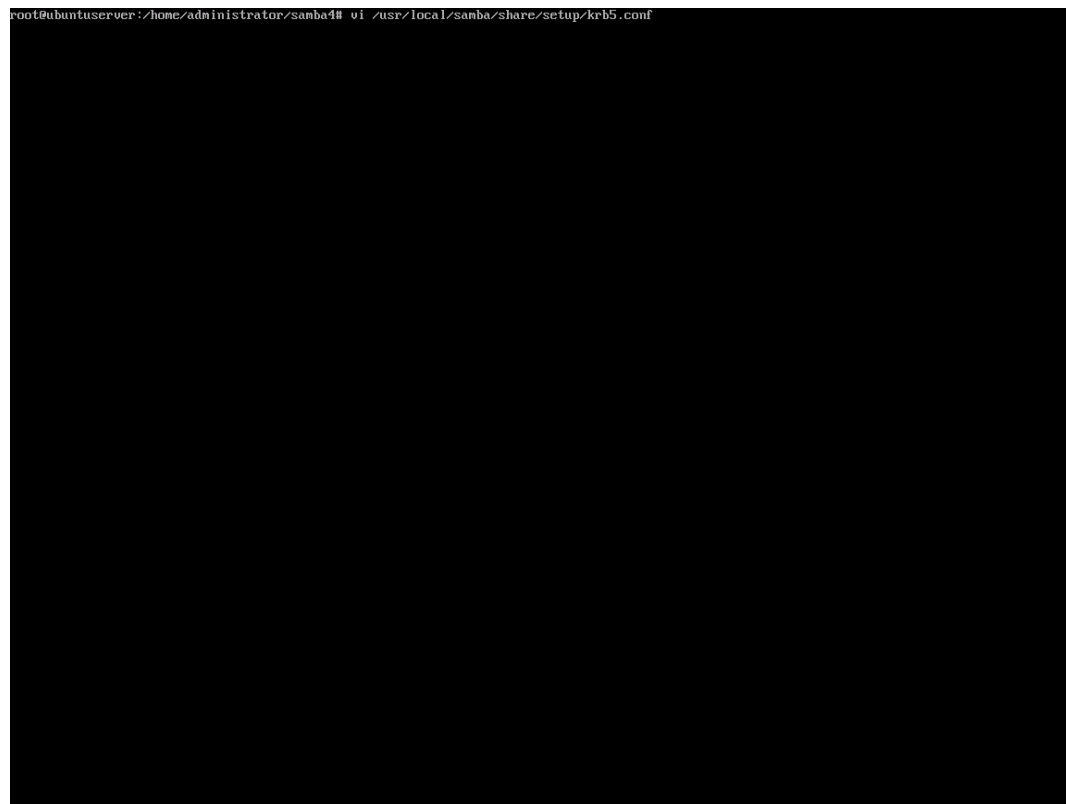


Figura 134 – Arquivo de Configuração do Kerberos



Figura 135 – Arquivo de Configuração do Kerberos com o Domínio

```
[libdefaults]
    default_realm = MONOGRAFIA.LOCAL_
    dns_lookup_realm = false
    dns_lookup_kdc = true
```

-- INSERT --

2,34-41 all

Figura 136 – Confirmação de Funcionamento do Kerberos

```
root@ubuntuserver:/home/administrator/samba4# kinit administrator@MONOGRAFIA.LOCAL
Password for administrator@MONOGRAFIA.LOCAL:
kinit: Preauthentication failed while getting initial credentials
root@ubuntuserver:/home/administrator/samba4# kinit administrator@MONOGRAFIA.LOCAL
Password for administrator@MONOGRAFIA.LOCAL:
Warning: Your password will expire in 41 days on Sat 08 Nov 2014 09:00:40 AM BRST
root@ubuntuserver:/home/administrator/samba4# klist -e
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@MONOGRAFIA.LOCAL

Valid starting     Expires            Service principal
09/27/2014 22:54:56  09/28/2014 08:54:56  krbtgt/MONOGRAFIA.LOCAL@MONOGRAFIA.LOCAL
    renew until 09/28/2014 22:54:53, Etype (skey, tkt): arcfour-hmac, arcfour-hmac
root@ubuntuserver:/home/administrator/samba4#
```

5.2.3.11 Pastas para Usuários

É muito importante criar a pasta *Users* no domínio para que o perfil dos novos usuários sejam criados organizadamente. Para isso deve-se executar a seguinte sequência de comandos:

```
mkdir -m 770 /Users
```

```
chmod g+s /Users
```

```
chown root:users /Users
```

Após criar as pastas para armazenamento é preciso configurar o arquivo de configuração do samba para que o sistema entenda que os novos perfis devem ser criados no local determinado. O comando para editar o arquivo de configuração é: *vi /usr/local/samba/etc/smb.conf*. Ao entrar no arquivo de configuração é preciso acrescentar as seguintes linhas:

```
[Users]
```

```
directory_mode: parameter = 0700
```

```
read only = no
```

```
path = /Users
```

```
csc policy = documents
```

Figura 137 – Comando para Edição de Smb.conf

```

root@ubuntuuserver:/home/administrator/samba4# kinit administrator@MONOGRAFIA.LOCAL
Password for administrator@MONOGRAFIA.LOCAL:
kinit: Preauthentication failed while getting initial credentials
root@ubuntuuserver:/home/administrator/samba4# kinit administrator@MONOGRAFIA.LOCAL
Password for administrator@MONOGRAFIA.LOCAL:
Warning: Your password will expire in 41 days on Sat 08 Nov 2014 09:00:40 AM BRST
root@ubuntuuserver:/home/administrator/samba4# klist -e
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@MONOGRAFIA.LOCAL

Valid starting     Expires            Service principal
09/27/2014 22:54:56  09/28/2014 00:54:56  krbtgt/MONOGRAFIA.LOCAL@MONOGRAFIA.LOCAL
           renew until 09/28/2014 22:54:53, Etype (skey, tkt): arcfour-hmac, arcfour-hmac
root@ubuntuuserver:/home/administrator/samba4# mkdir -m 770 /Users
root@ubuntuuserver:/home/administrator/samba4# chmod g+s /Users
root@ubuntuuserver:/home/administrator/samba4# chown root:users /Users
root@ubuntuuserver:/home/administrator/samba4# vi /usr/local/samba/etc/smb.conf

```

Figura 138 – Arquivo de Configuração do SAMBA

```

# Global parameters
[global]
    workgroup = MONOGRAFIA
    realm = monografia.local
    netbios name = UBUNTUSERVER
    server role = active directory domain controller
    dns forwarder = 8.8.8.8

[netlogon]
    path = /usr/local/samba/var/locks/sysvol/monografia.local/scripts
    read only = No

[sysvol]
    path = /usr/local/samba/var/locks/sysvol
    read only = No

```


Figura 139 – Arquivo de Configuração do SAMBA com Parâmetro de Usuários

```
[global]
    workgroup = MONOGRAFIA
    realm = monografia.local
    netbios name = UBUNTUSERVER
    server role = active directory domain controller
    dns forwarder = 8.8.8.8

[netlogon]
    path = /usr/local/samba/var/locks/sysvol/monografia.local/scripts
    read only = No

[sysvol]
    path = /usr/local/samba/var/locks/sysvol
    read only = No

[Users]
    directory_mode: parameter = 0700
    read only = no
    path = /Users
    csc_policy = documents

"/usr/local/samba/etc/smb.conf" 21L, 440C written
root@ubuntuuserver:/home/administrator/samba4#
```

5.2.3.12 Senha de Administrador

Após criada a senha do administrador do domínio é preciso fazer com que ela não expire usando o comando `/usr/local/samba/bin/samba-tool user setexpiry administrator --noexpiry`.

Figura 140 – Retirar Regra de Expiração de Senha

```

realm = monografia.local
netbios name = UBUNTUSERVER
server role = active directory domain controller
dns forwarder = 8.8.8.8

[netlogon]
path = /usr/local/samba/var/locks/sysvol/monografia.local/scripts
read only = No

[sysvol]
path = /usr/local/samba/var/locks/sysvol
read only = No

[Users]
directory_mode: parameter = 0700
read only = no
path = /Users
csc_policy = documents

"/usr/local/samba/etc/smb.conf" 21L, 440C written
root@ubuntuserver:/home/administrator/samba4# /usr/local/samba/bin/samba-tool user setexpiry administrator --noexpiry
Expiry for user 'administrator' disabled.
root@ubuntuserver:/home/administrator/samba4#

```

5.2.3.13 Configurar IP da Máquina Cliente

Para que computadores sejam adicionados no domínio, primeiro é preciso colocar o computador que entrará no domínio, cliente, na mesma rede em que o servidor está. Para este computador cliente foi criada uma maquina virtual com o Windows 8.1 da Microsoft. Para o caso deste trabalho é preciso colocar um IP estático devido a nenhum servidor DHCP ter sido configurado na rede. O IP escolhido foi o 192.168.1.110. Para configura-lo é preciso entrar no painel de controle da máquina e acessar a central de rede e compartilhamento. Em seguida acessar a placa de rede e configurar as propriedades da placa no que diz respeito ao IPv4.

Para confirmar se a configuração está correta é preciso acessar o prompt de comando do computador e usar o comando ICMP para checar a comunicação entre as maquinas: *ping 192.168.1.100*.

Figura 141 – Central de Rede e Compartilhamento do Windows

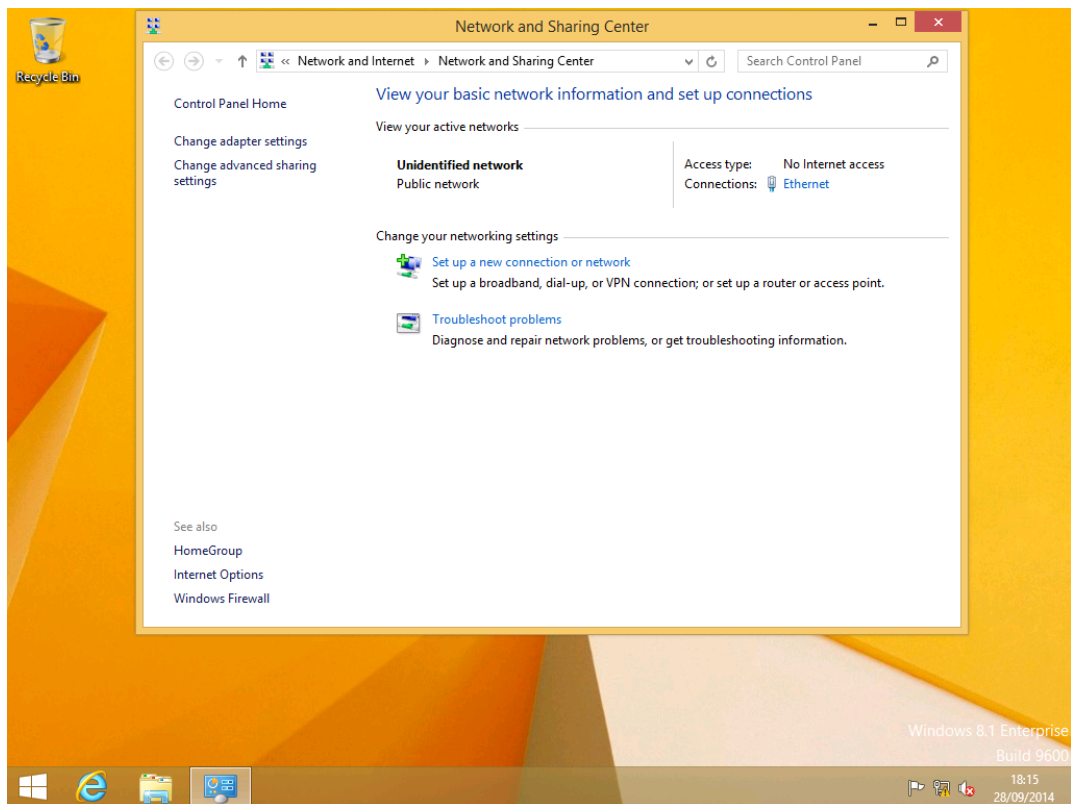


Figura 142 – Status de Conexão

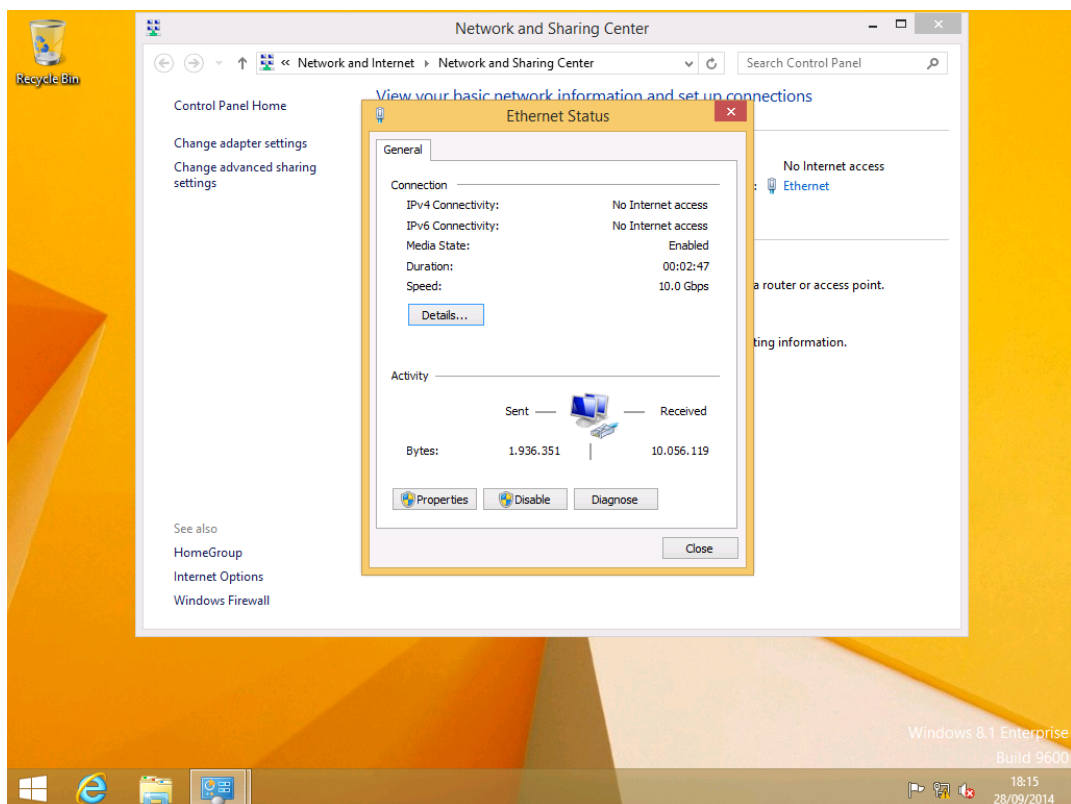


Figura 143 – Propriedades da Interface de Rede

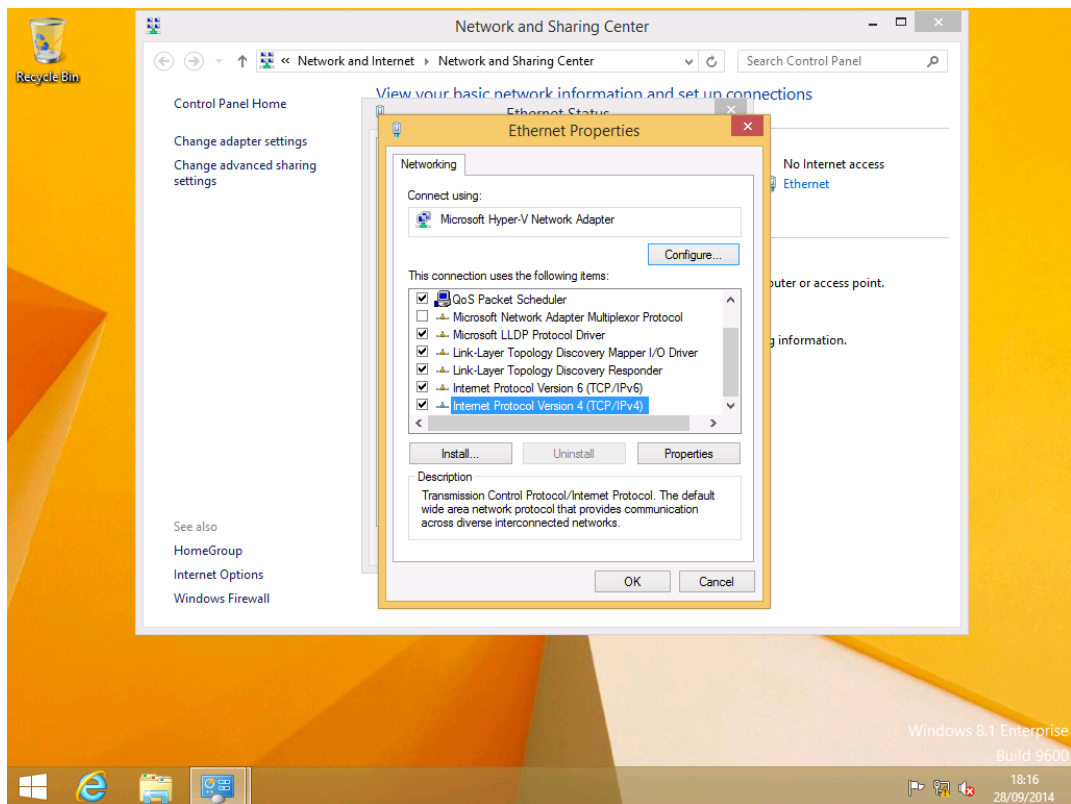


Figura 144 – Inserção de IP Estático para a Estação de Trabalho

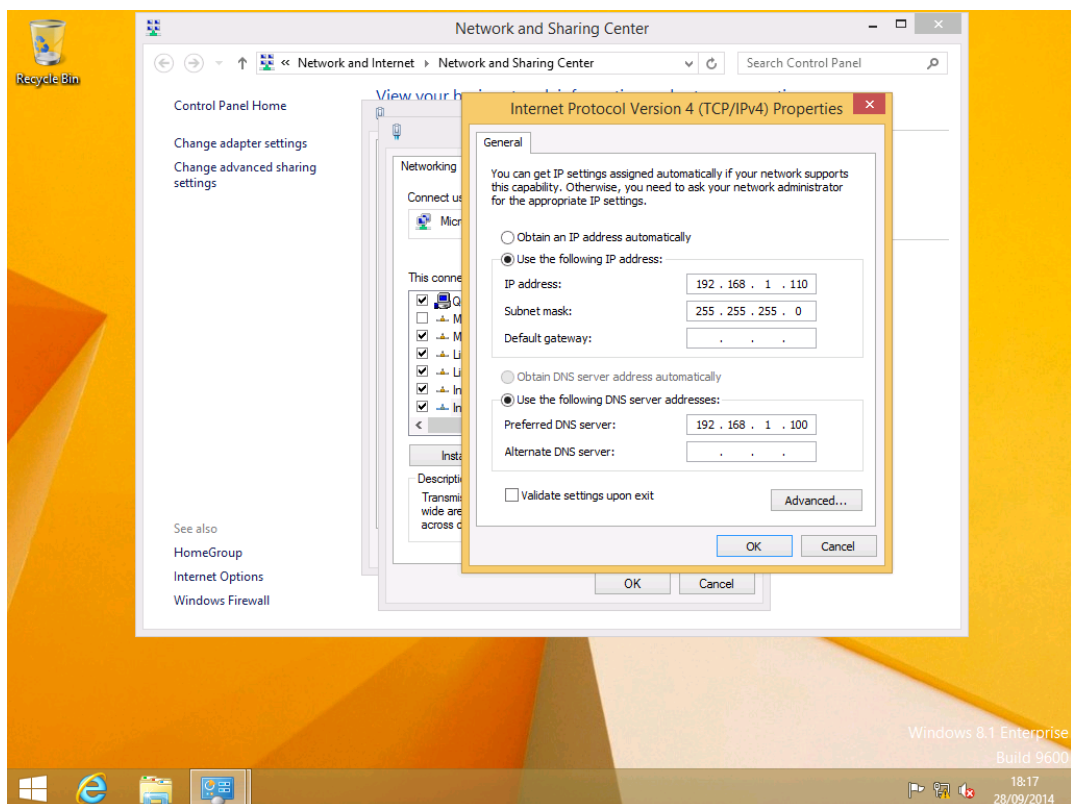


Figura 145 – Verificação de Comunicação de Rede com Servidor Linux

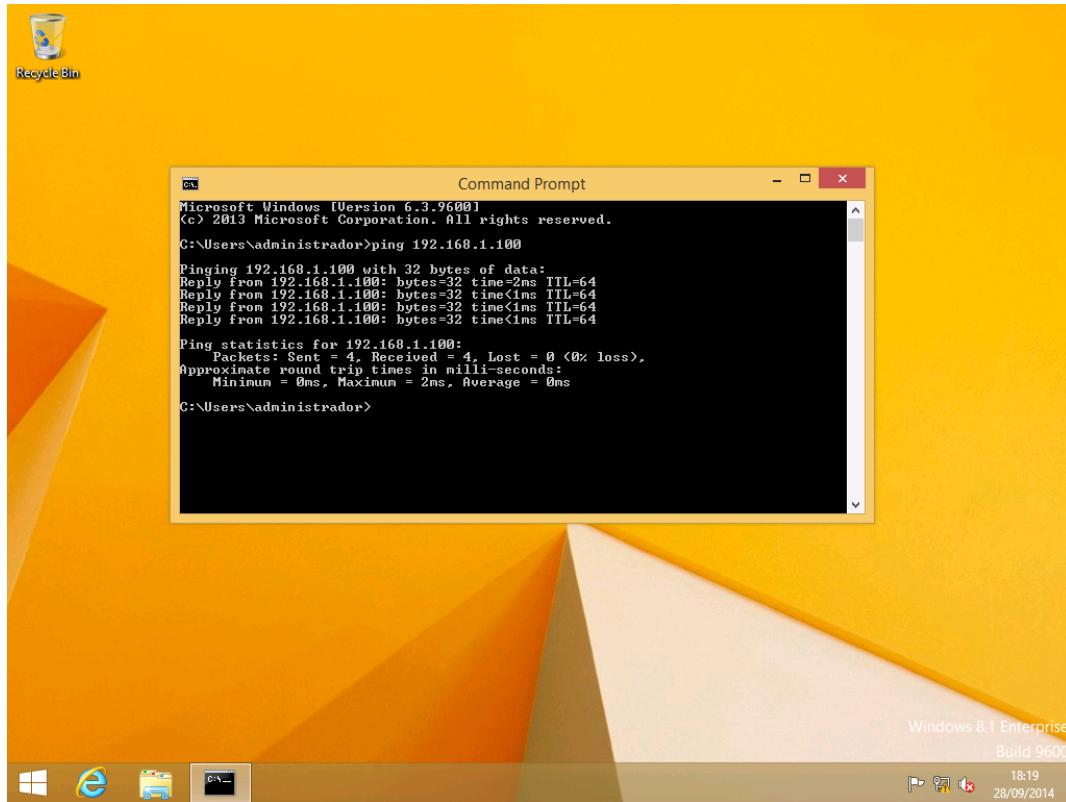


Figura 146 – Verificação de Comunicação de Rede com Estação de Trabalho

```

root@ubuntuserver:/home/administrator/samba4# ping 192.168.1.110
PING 192.168.1.110 (192.168.1.110) 56(84) bytes of data:
64 bytes from 192.168.1.110: icmp_seq=1 ttl=128 time=0.679 ms
64 bytes from 192.168.1.110: icmp_seq=2 ttl=128 time=0.530 ms
64 bytes from 192.168.1.110: icmp_seq=3 ttl=128 time=0.562 ms
64 bytes from 192.168.1.110: icmp_seq=4 ttl=128 time=0.625 ms
64 bytes from 192.168.1.110: icmp_seq=5 ttl=128 time=0.463 ms
64 bytes from 192.168.1.110: icmp_seq=6 ttl=128 time=0.912 ms
64 bytes from 192.168.1.110: icmp_seq=7 ttl=128 time=0.581 ms
64 bytes from 192.168.1.110: icmp_seq=8 ttl=128 time=0.527 ms
^C
--- 192.168.1.110 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7012ms
rtt min/avg/max/mdev = 0.463/0.609/0.912/0.133 ms
root@ubuntuserver:/home/administrator/samba4# _
  
```

5.2.3.14 Adicionar Computador Cliente no Domínio

Da mesma forma que é feito no ambiente configurado com o controlador de domínio da Microsoft é preciso incluir o computador cliente manualmente no domínio. Para isso é preciso acessar as propriedades do computador e modificar as configurações. Ao acessar essas configurações é preciso colocar o nome do domínio completo no caso, *monografia.local*. Em seguida é preciso colocar as credenciais que foram configuradas no servidor para o administrador do domínio, no caso o *login* é *administrator* e a senha *P@ssw0rd*.

Figura 147 – Propriedades do Computador

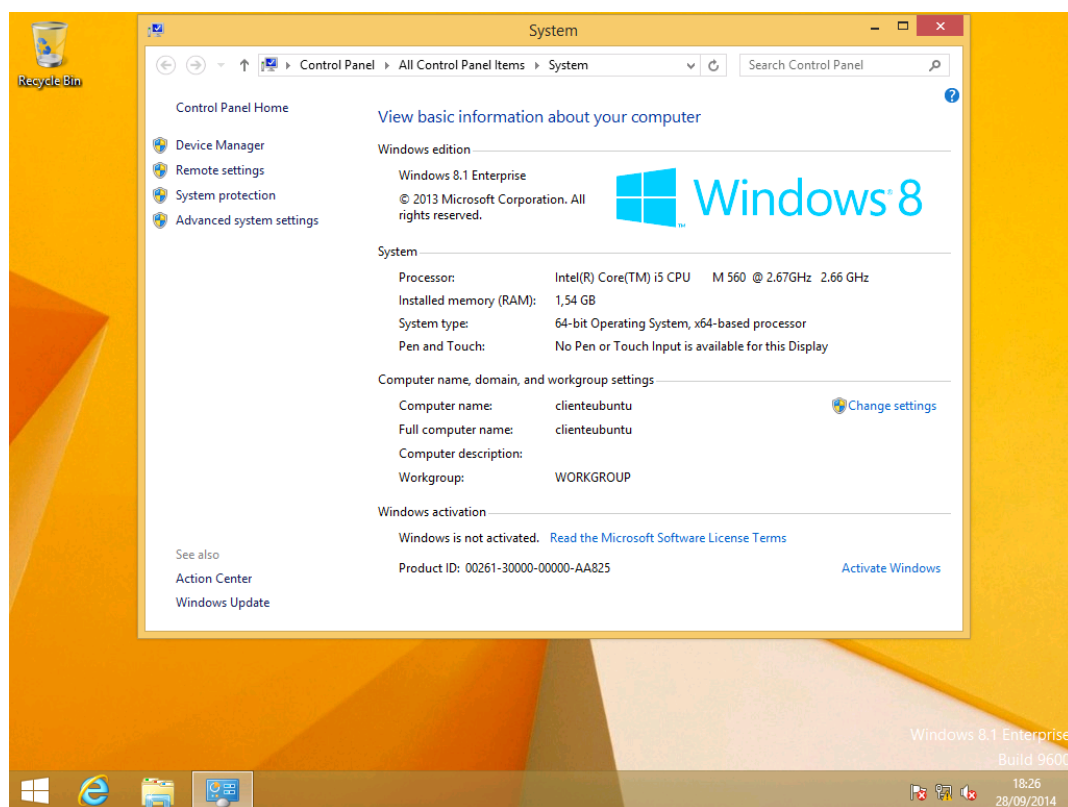


Figura 148 – Renomear Computador e Adicionar um Domínio

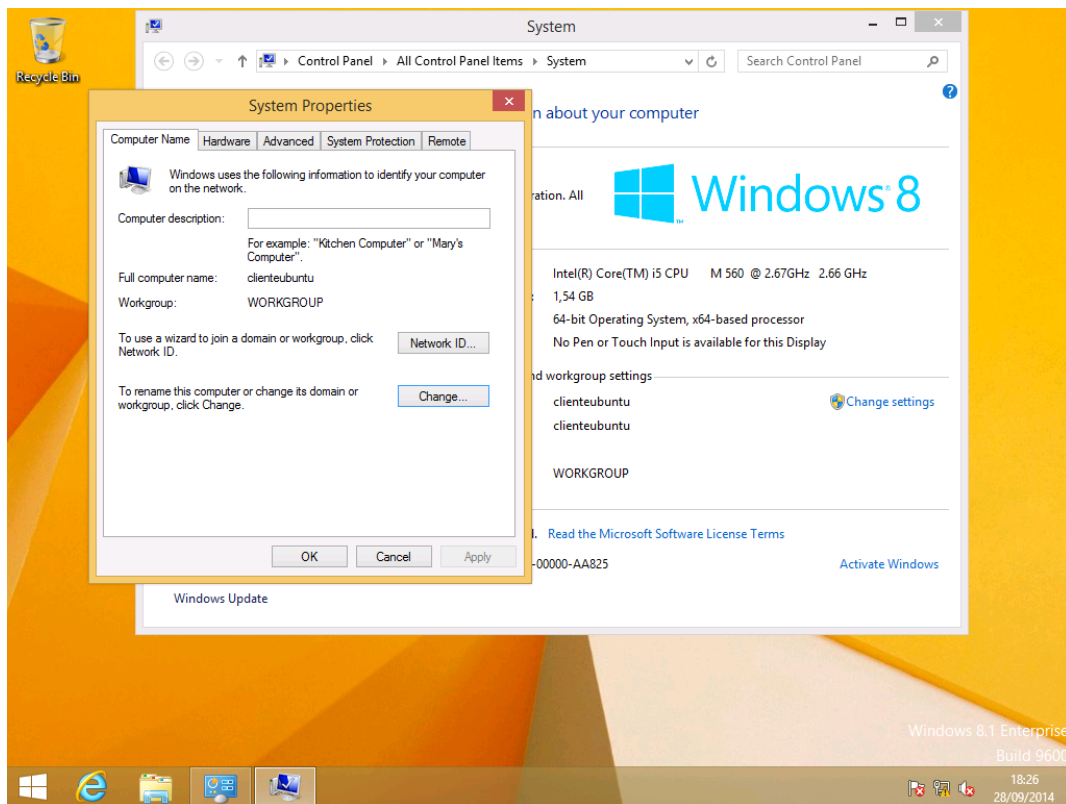


Figura 149 – Incluindo Computador no Domínio

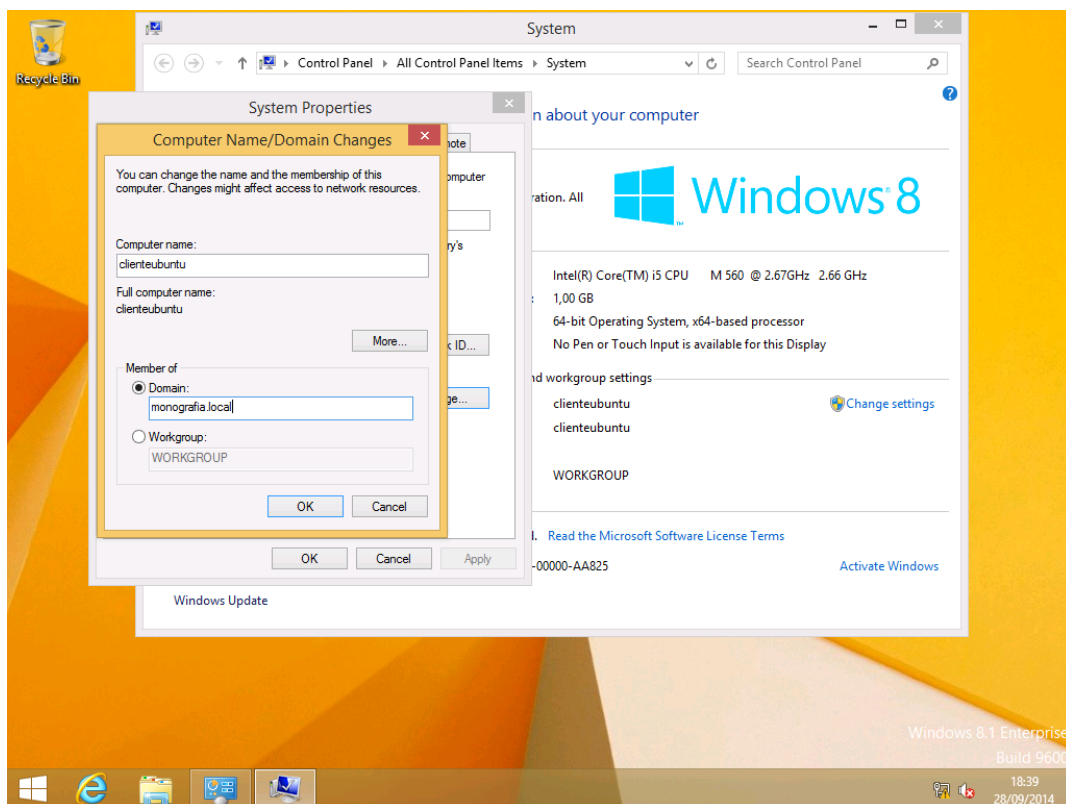


Figura 150 – Senha do Administrador do Domínio

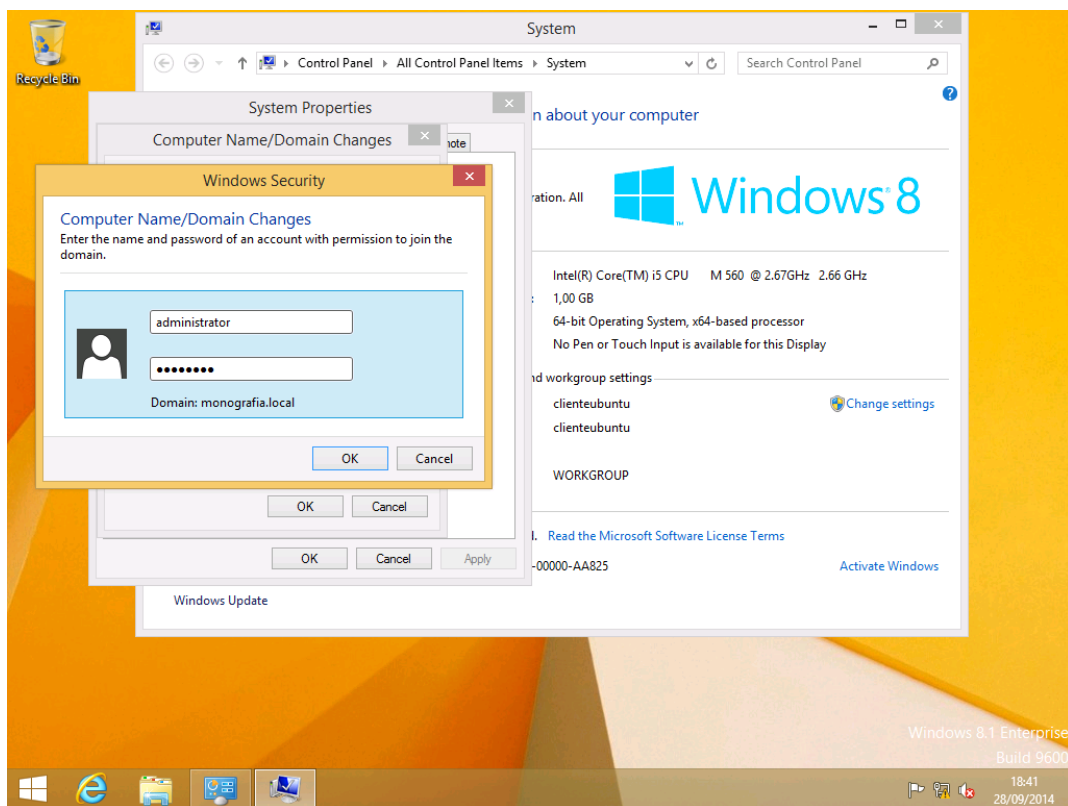
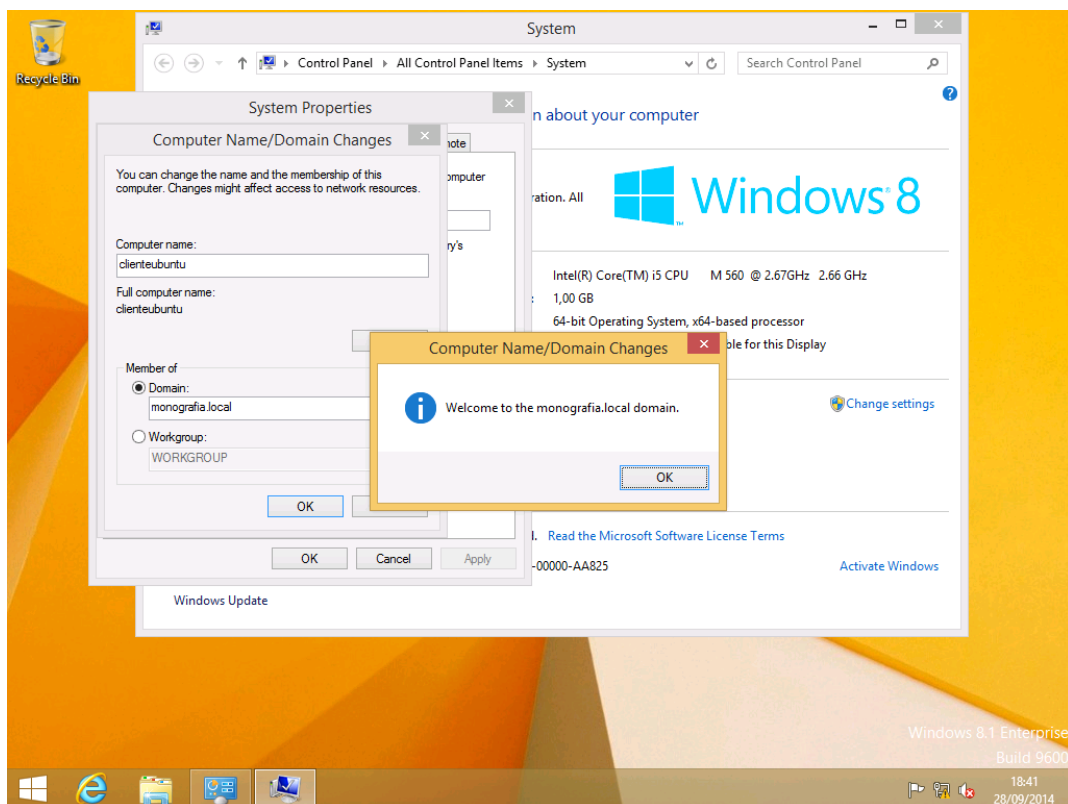


Figura 151 – Boas Vindas ao Domínio



5.2.3.15 Instalar as Ferramentas de Gerencia do Domínio

Agora que o computador cliente está no domínio, é preciso fazer acessá-lo usando o único usuário criado no domínio que é o *administrator.n*. Para isso é preciso entrar com o *login* monografia\administrator e senha.

Uma vez dentro da máquina é preciso instalar um pacote de línguas suportado pela ferramenta de administração, para isso é preciso fazer a atualização do sistema em seguida entrar nas configurações do computador e fazer o download do pacote de línguas escolhido.

Somente após a instalação do pacote de línguas, no caso o escolhido foi o pacote de português, é possível instalar uma atualização que adiciona ferramentas administrativas para gerencia de controlador de domínio remotamente. Para fazer o download da atualização é preciso acessar o sítio <http://www.microsoft.com/en-ca/download/details.aspx?id=39296> fazer o download compatível com a versão do Windows e instala-la.

Figura 152 – Acesso à Estação de Trabalho

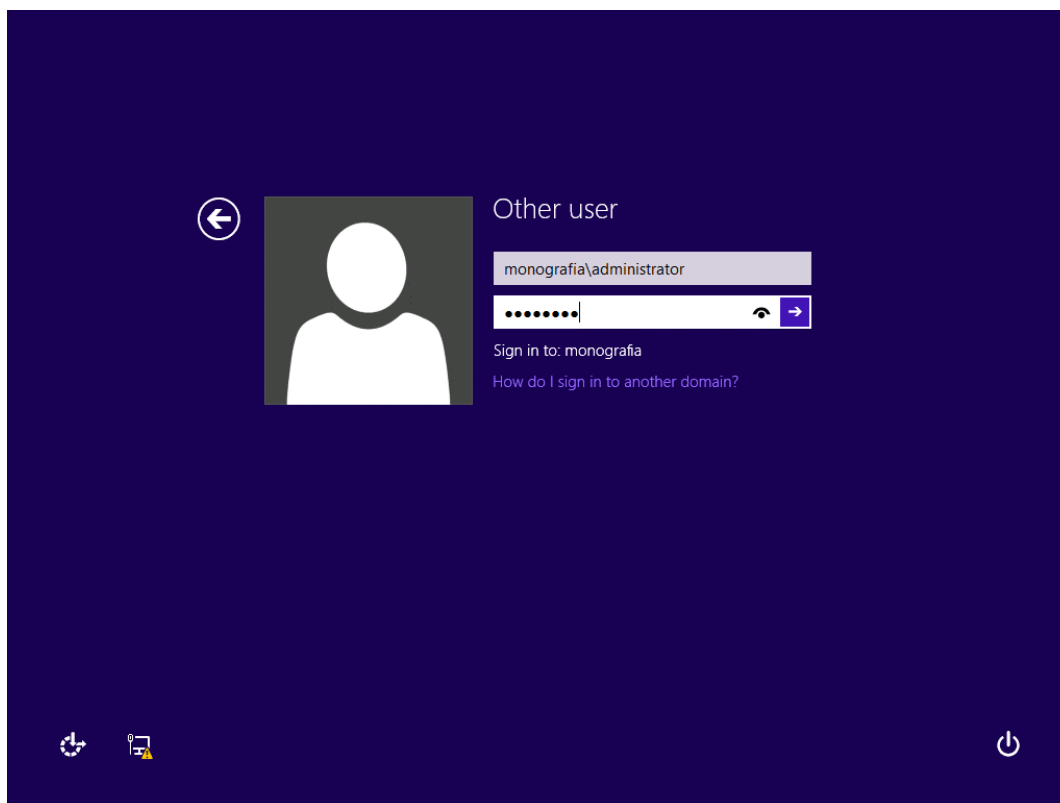


Figura 153 – Opções do Computador



Figura 154 – Configurações do Computador

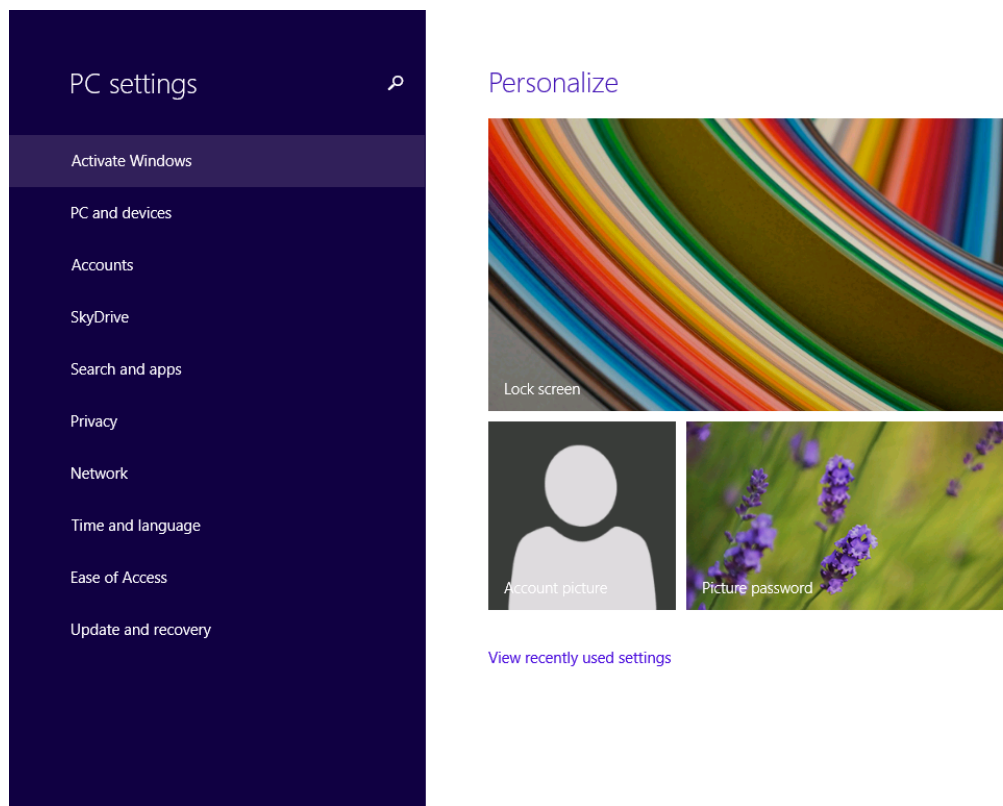


Figura 155 – Adicionando a Língua Portuguesa

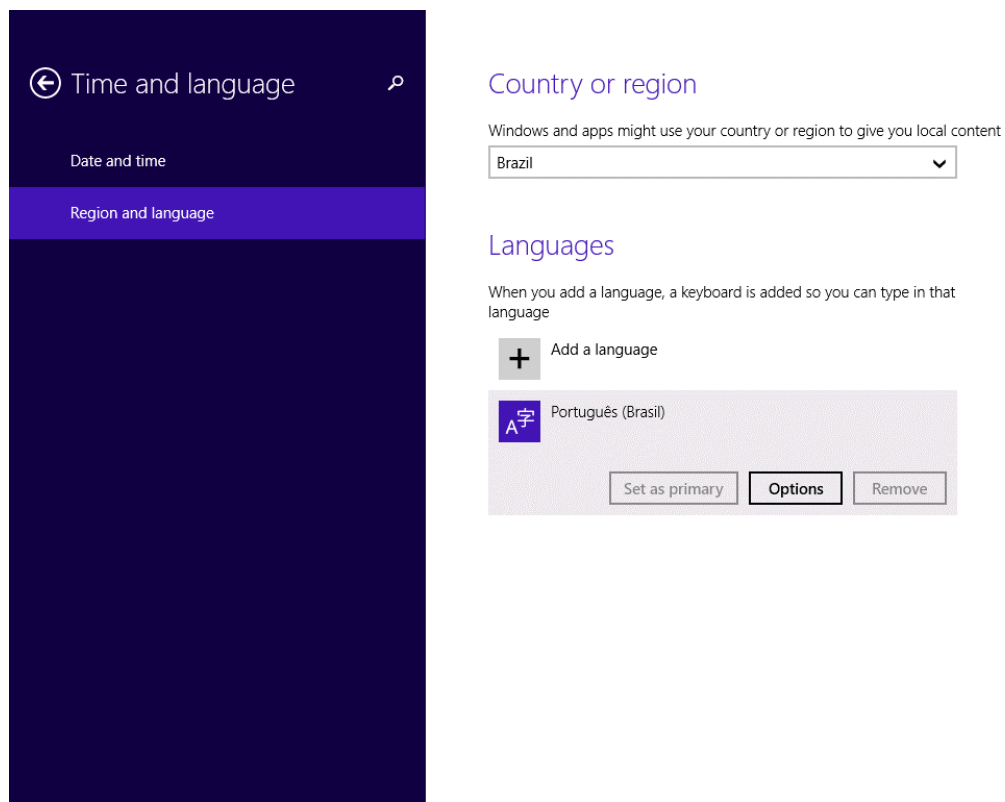


Figura 156 –Download das Ferramentas de Administração Remota do Servidor

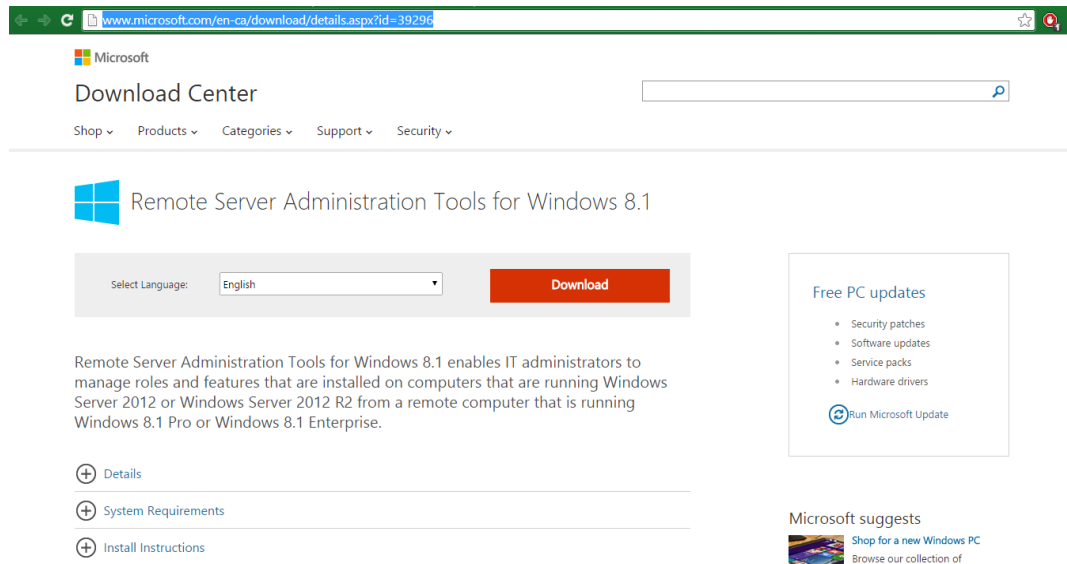


Figura 157 – Painel de Controle

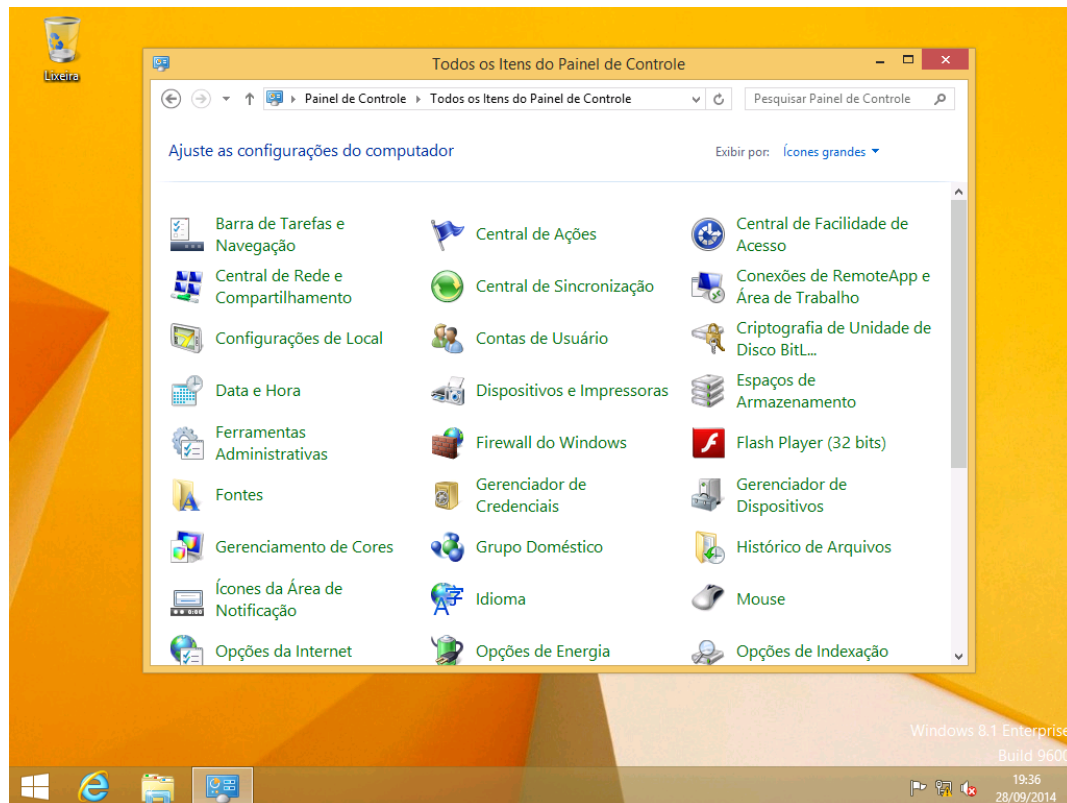


Figura 158 – Ferramentas Administrativas do Computador

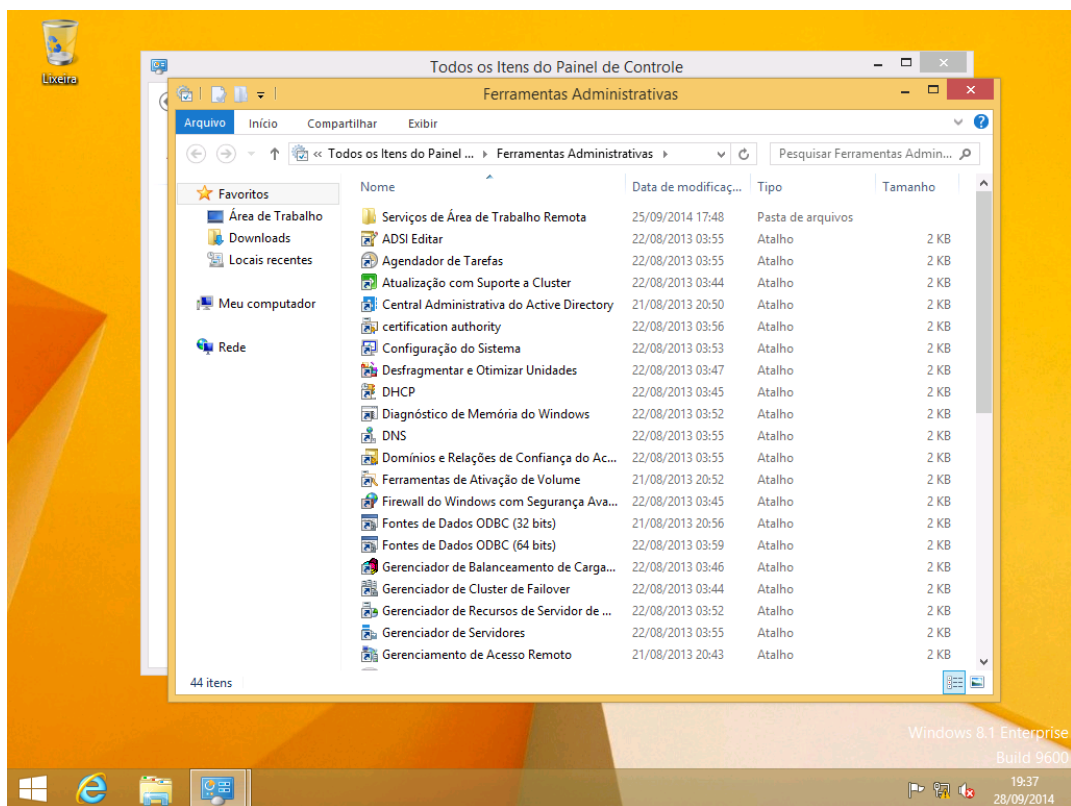


Figura 159 – Usuários e Computadores do AD

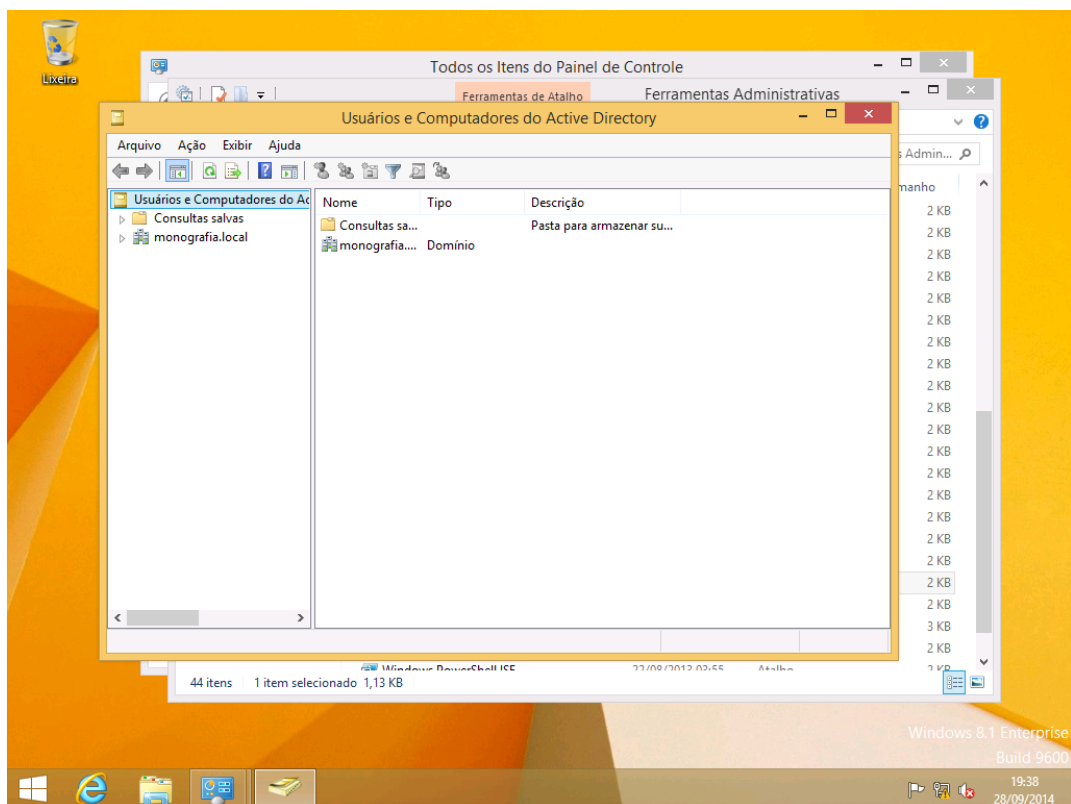
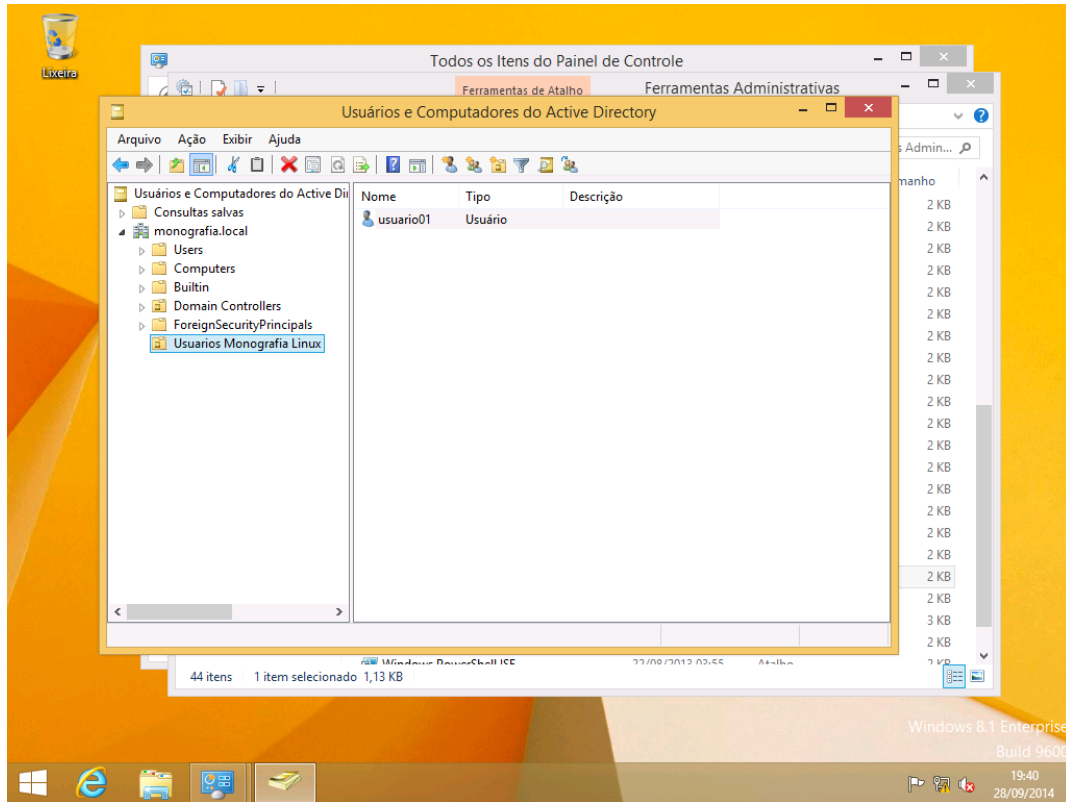


Figura 160 – Unidade Organizacional para Usuários do Domínio



5.2.3.16 Autenticação no Domínio

Para fazer a autenticação no domínio criado com o SAMBA no Linux, é preciso criar um usuário no sistema Linux em seguida no programa SAMBA. Usando o comando *adduser* cria-se o usuário no sistema Linux e o comando *smbpasswd -a* cria-se o usuário no SAMBA. Porém, como a administração do servidor Linux é feita remotamente usando um cliente Windows, podem-se usar as ferramentas de administração para criação de usuário. Uma vez criado o usuário é possível fazer acesso ao domínio com autenticação de senha.

O primeiro passo a ser dado é acessar o cliente Windows, abrir o painel de controle e acessar as ferramentas administrativas. Em seguida é preciso acessar o a ferramenta de administração “Usuários e Computadores do Active Directory”, clicar com o botão direito no nome do domínio e criar uma nova unidade organizacional. Uma vez criado a unidade organizacional “usuários ubuntu” é preciso

clicar no ícone de criar usuários e adicionar um novo usuário no domínio. Para este trabalho foram criados os usuário: usuario01, usuario02, usuario03, usuario04, usuario05 e usuario06. Os usuários 01 e 02 foram incluídos no grupo de Marketing, 03 e 04 no grupo de Recursos Humanos e 05 e 06 no grupo de Suporte Técnico.

Figura 161 – Painel de Controle

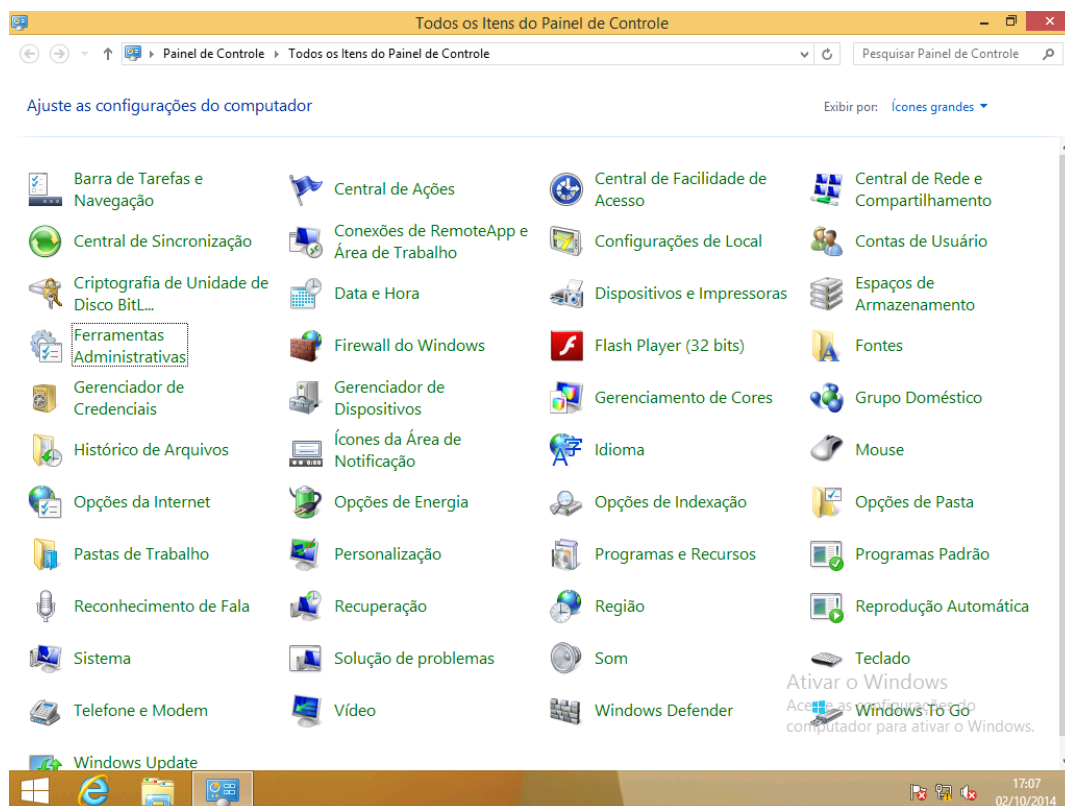


Figura 162 – Ferramentas Administrativas

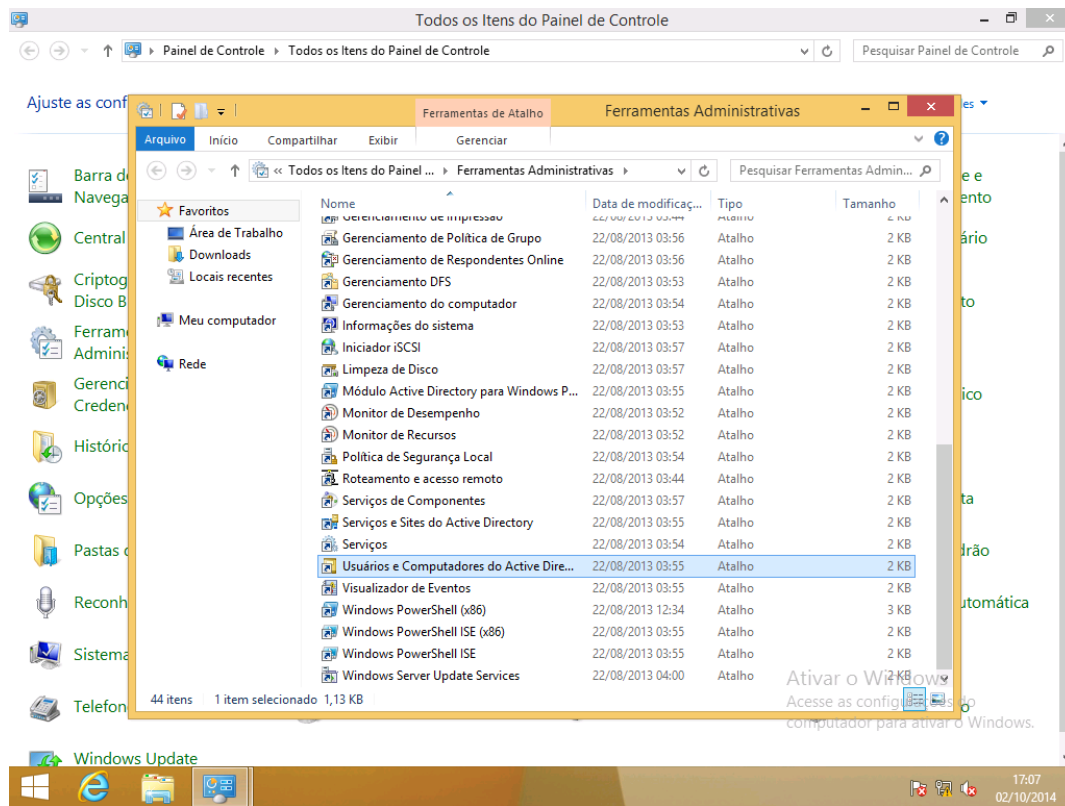


Figura 163 – Criação de Unidade Organizacional

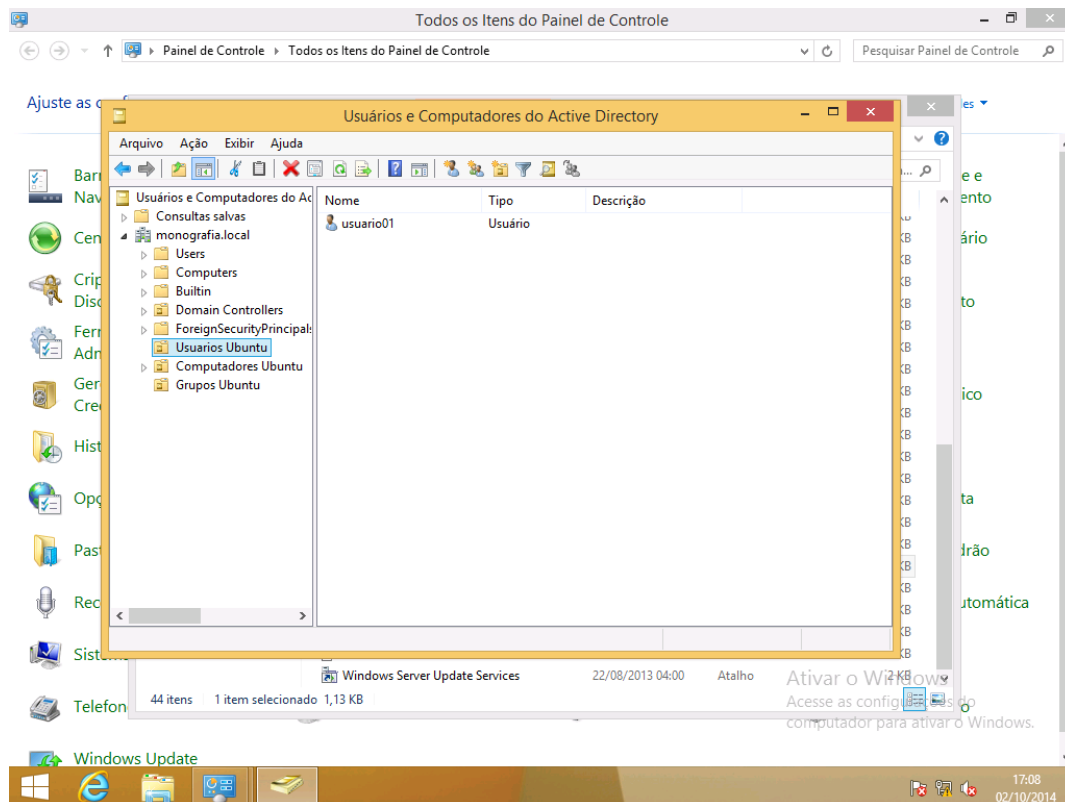


Figura 164 – Criação de Usuário

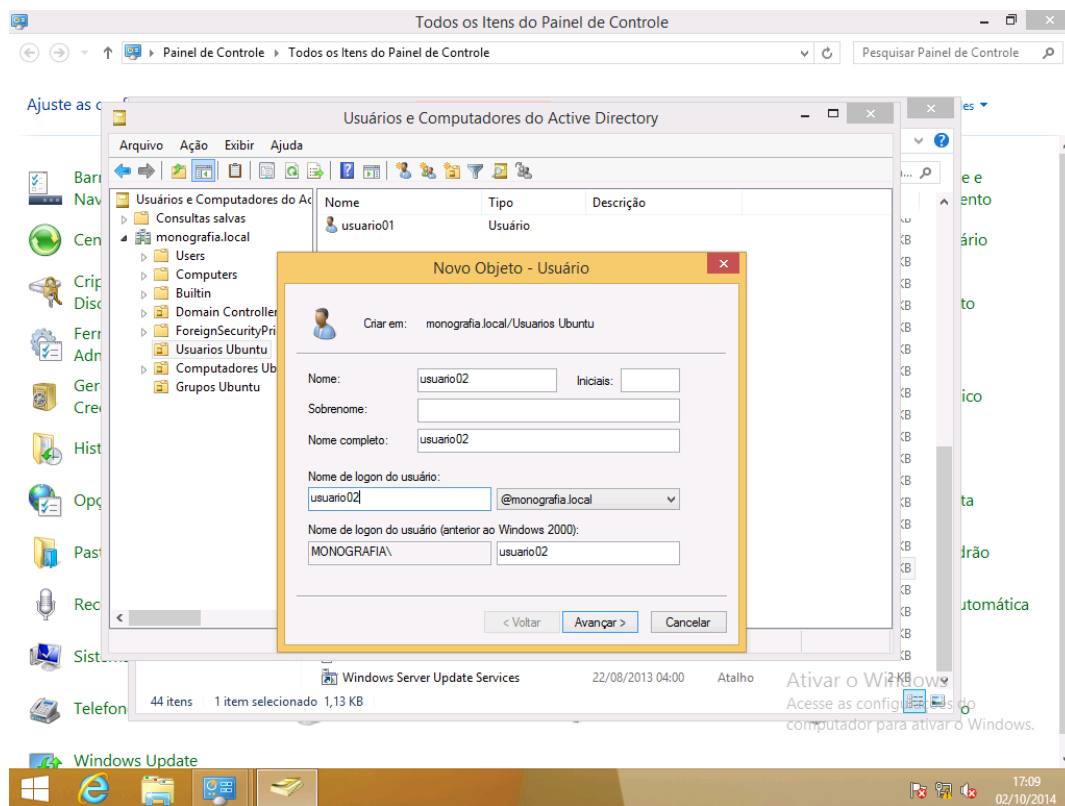


Figura 165 – Criação de Senha

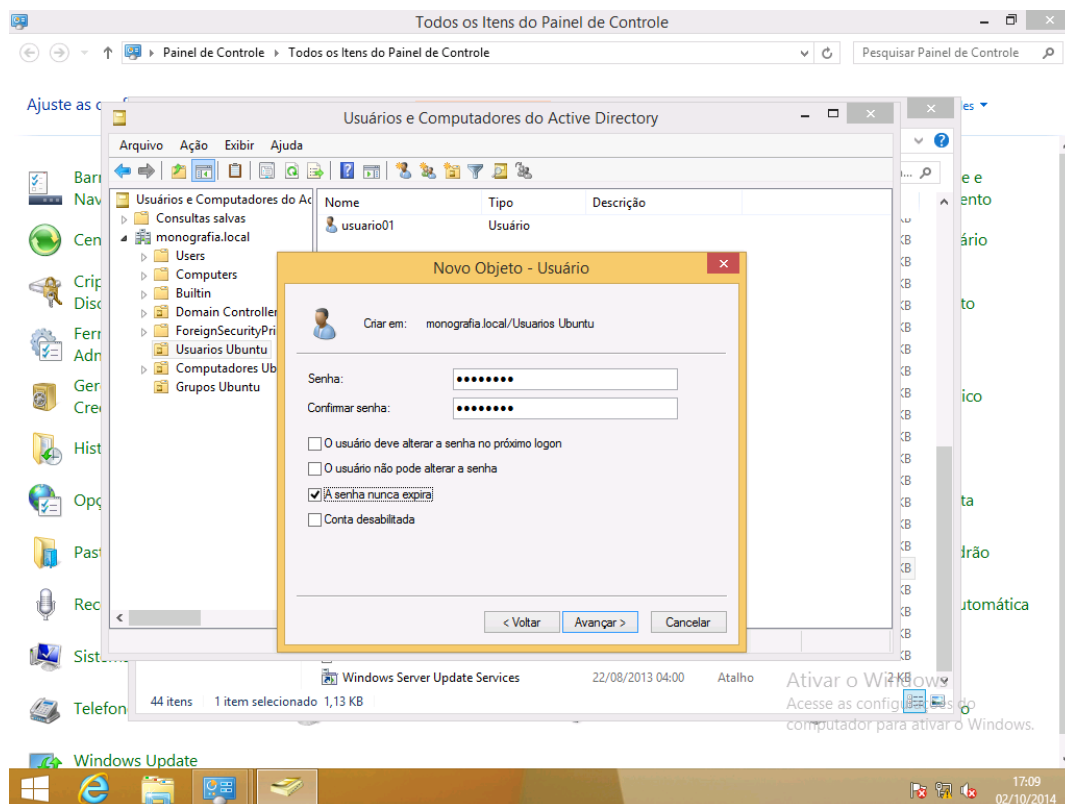


Figura 166 – Confirmação de Objeto Criado

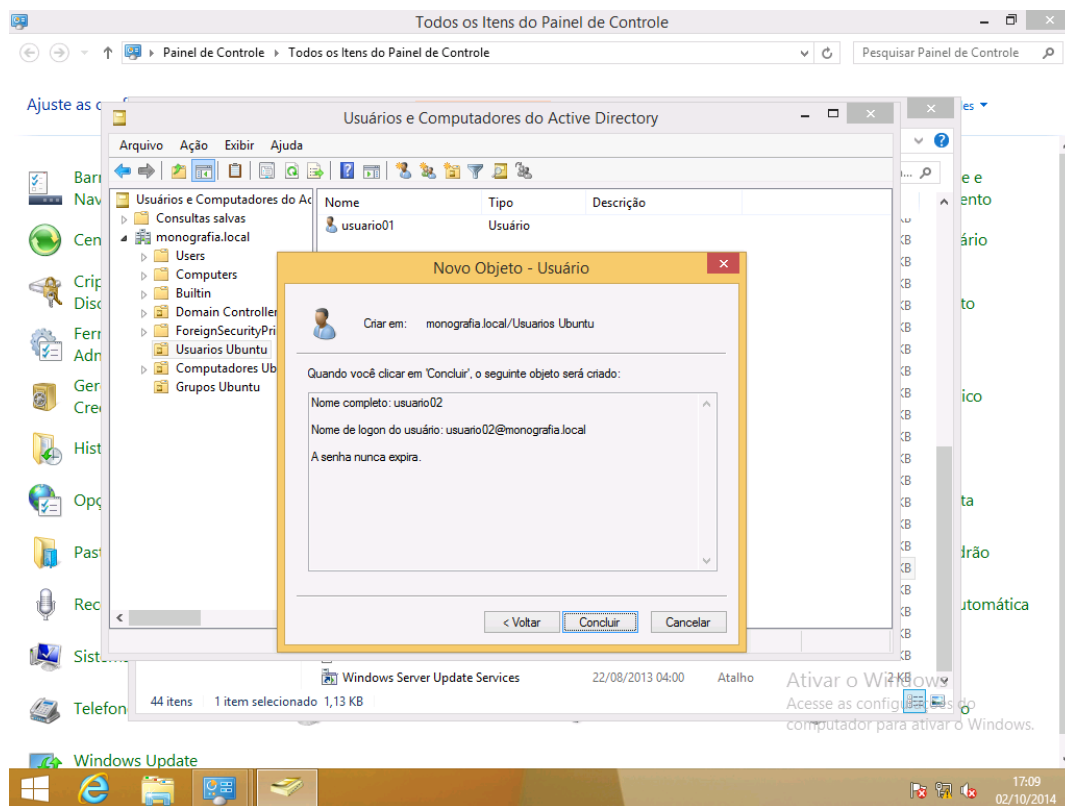


Figura 167 – Usuário Dois Criado no Grupo

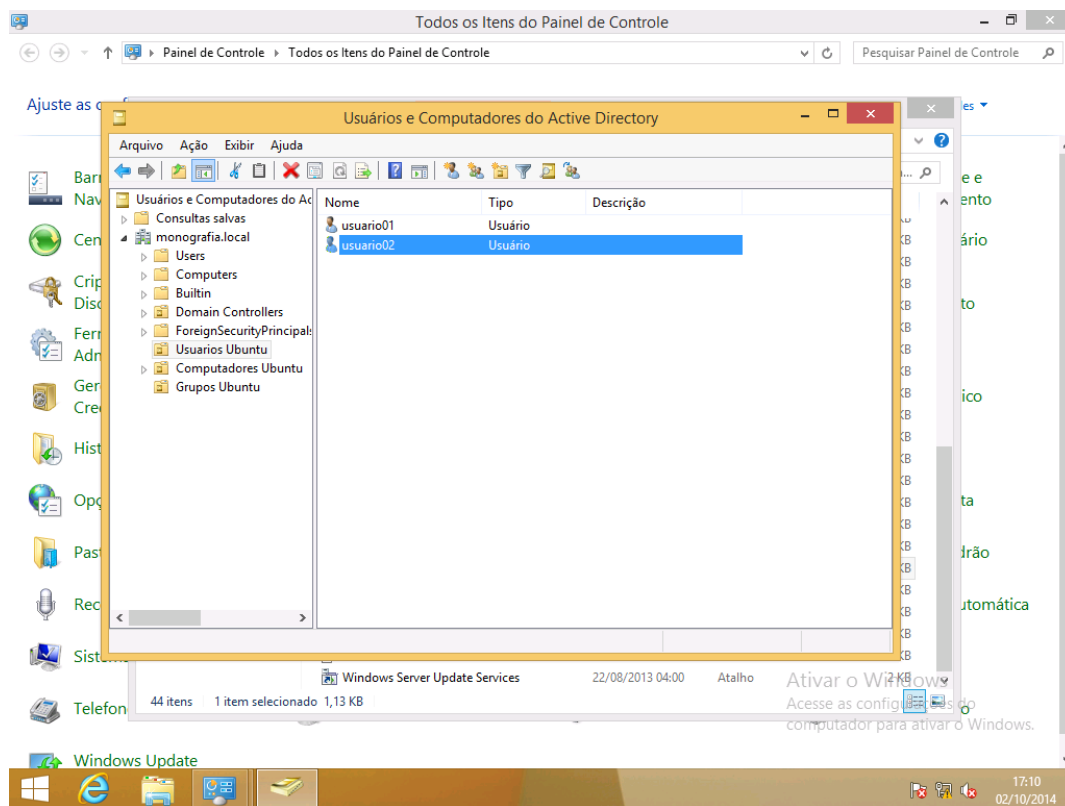


Figura 168 – Usuários de Um a Seis Criados no Grupo

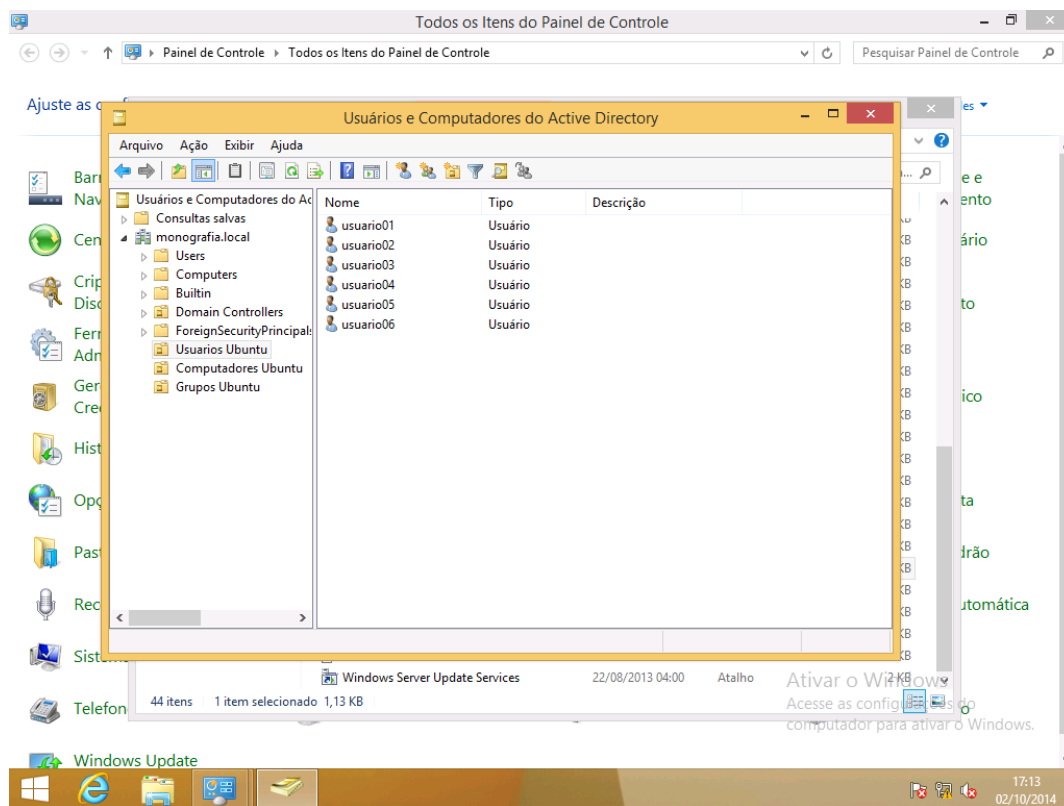


Figura 169 – Criando Grupo de Segurança

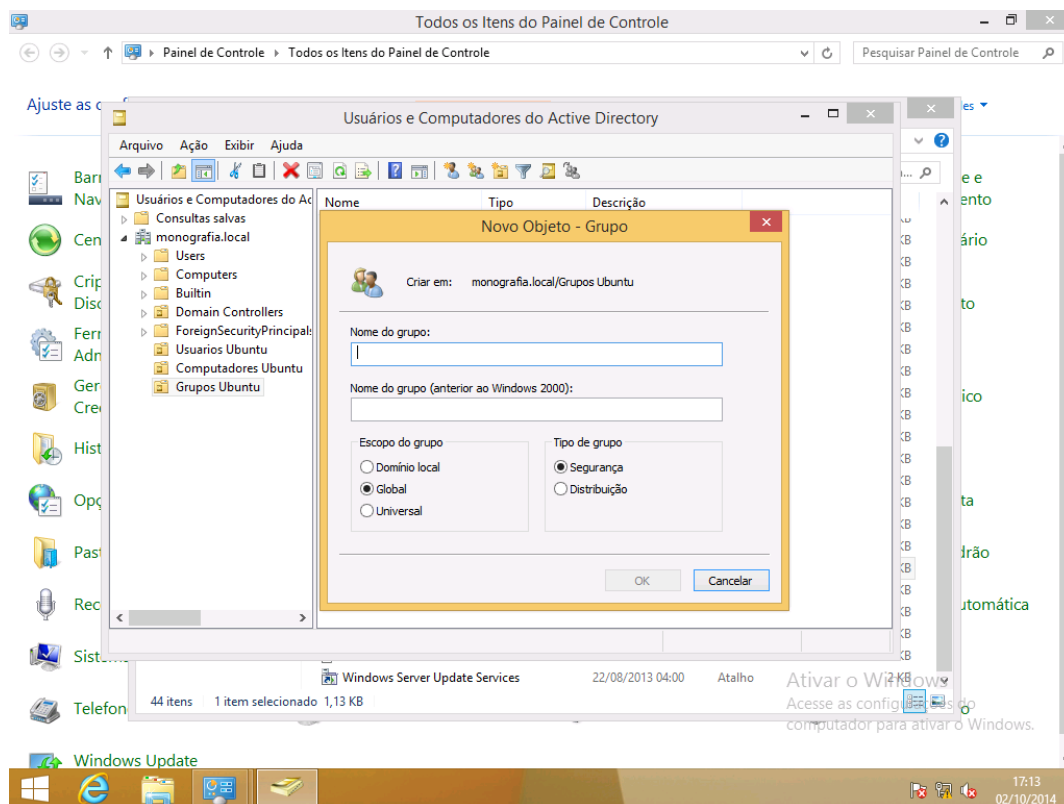


Figura 170 – Grupo do Suporte Técnico

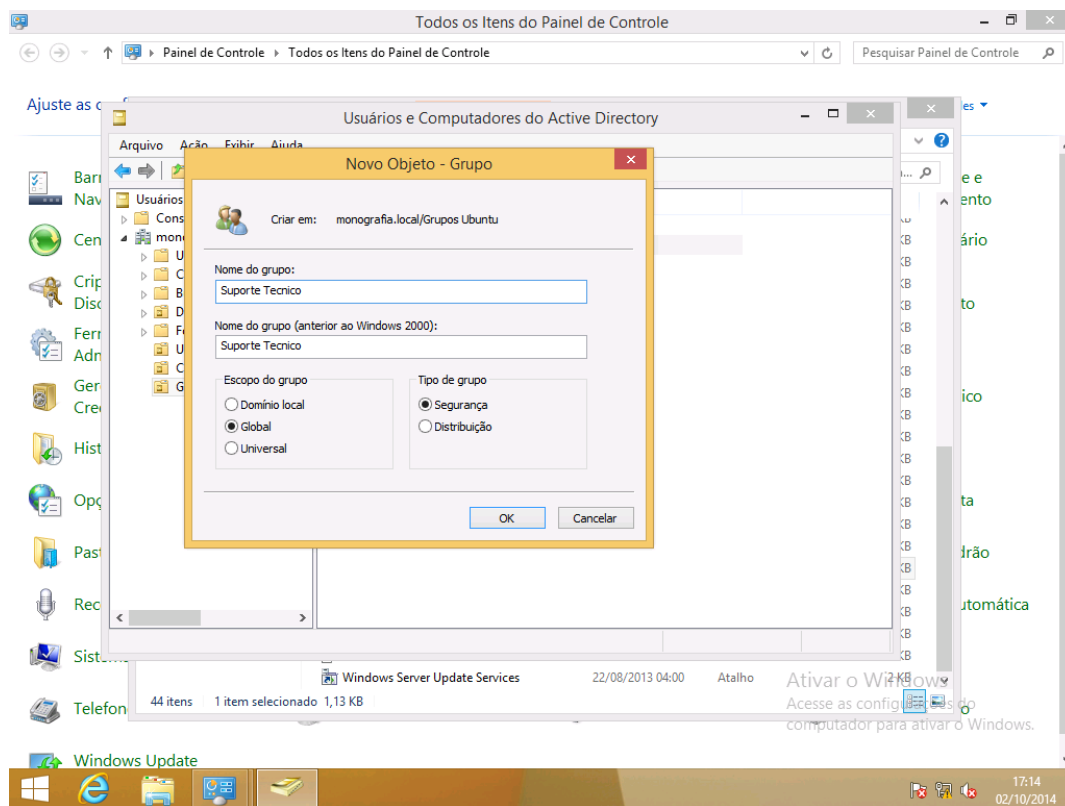


Figura 171 – Grupos Criados

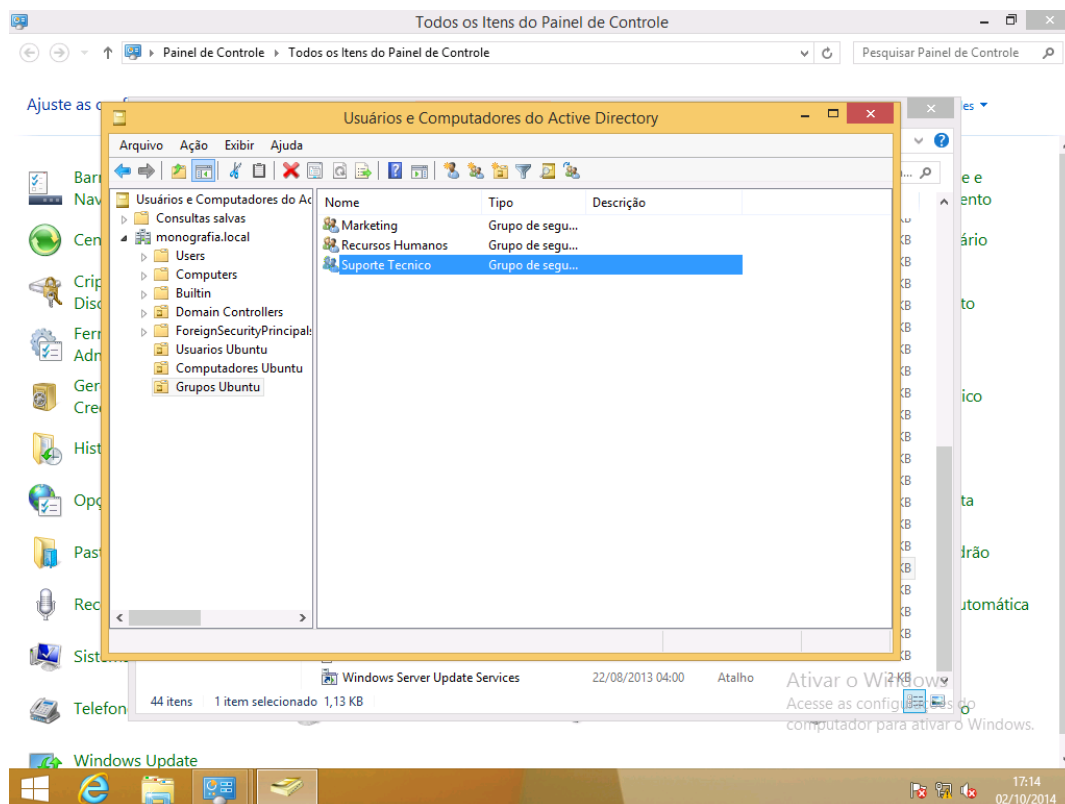


Figura 172 – Usuários Adicionados no Grupo Marketing

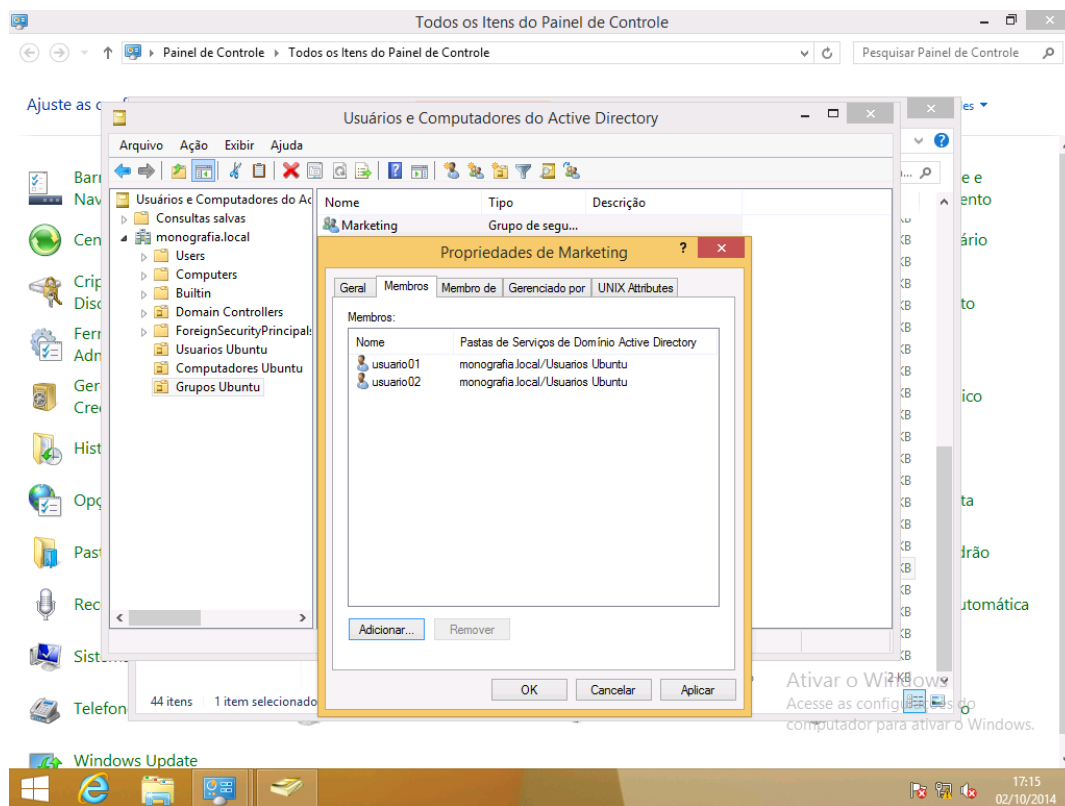


Figura 173 – Usuários Adicionados no Grupo Recursos Humanos

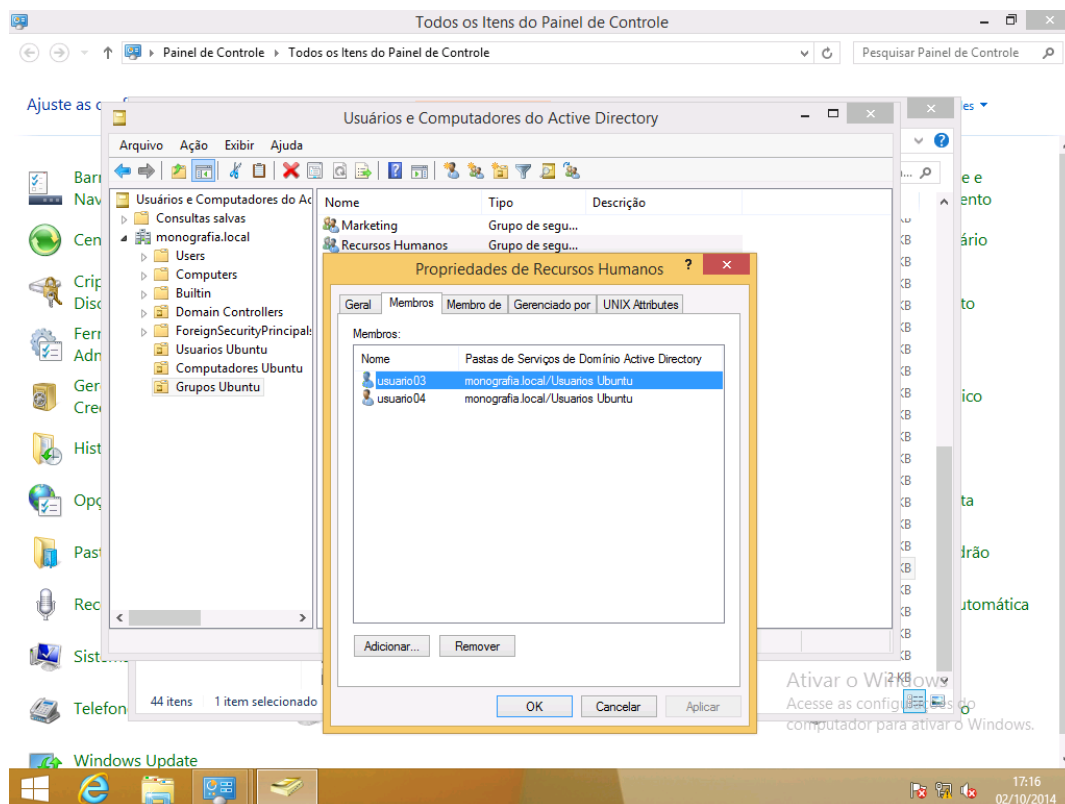


Figura 174 – Usuários Adicionados no Grupo Suporte técnico

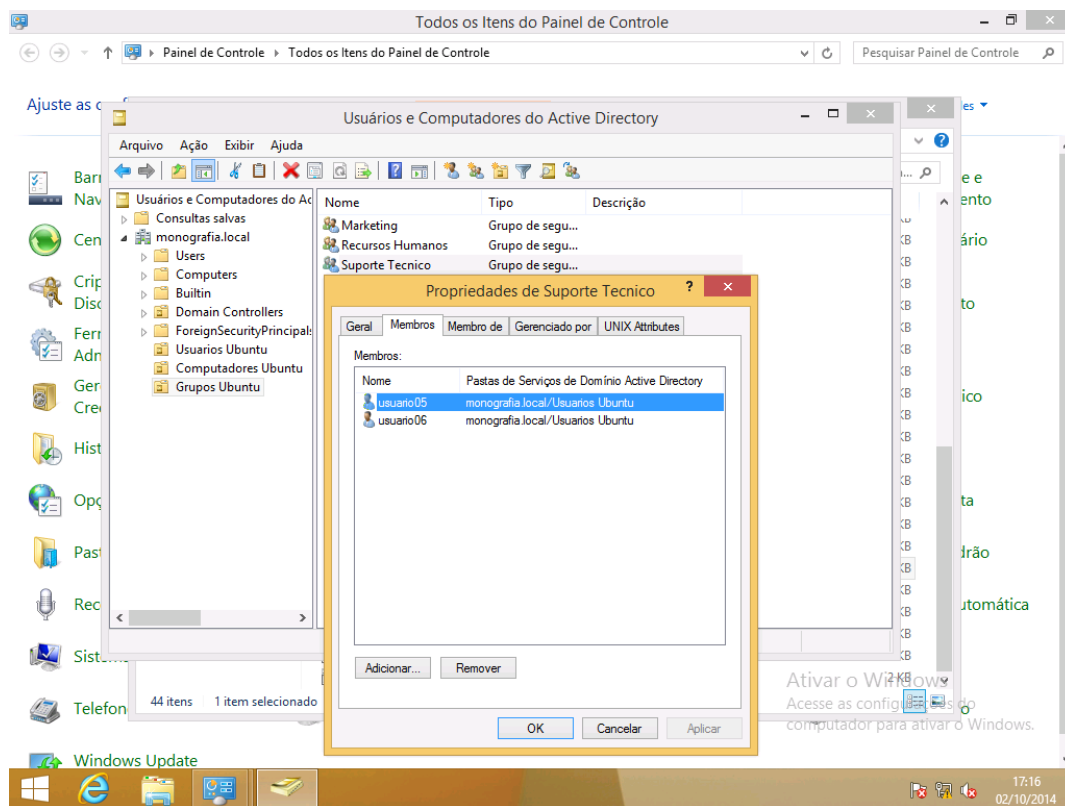


Figura 175 – Acesso ao Domínio pelo Usuário 01

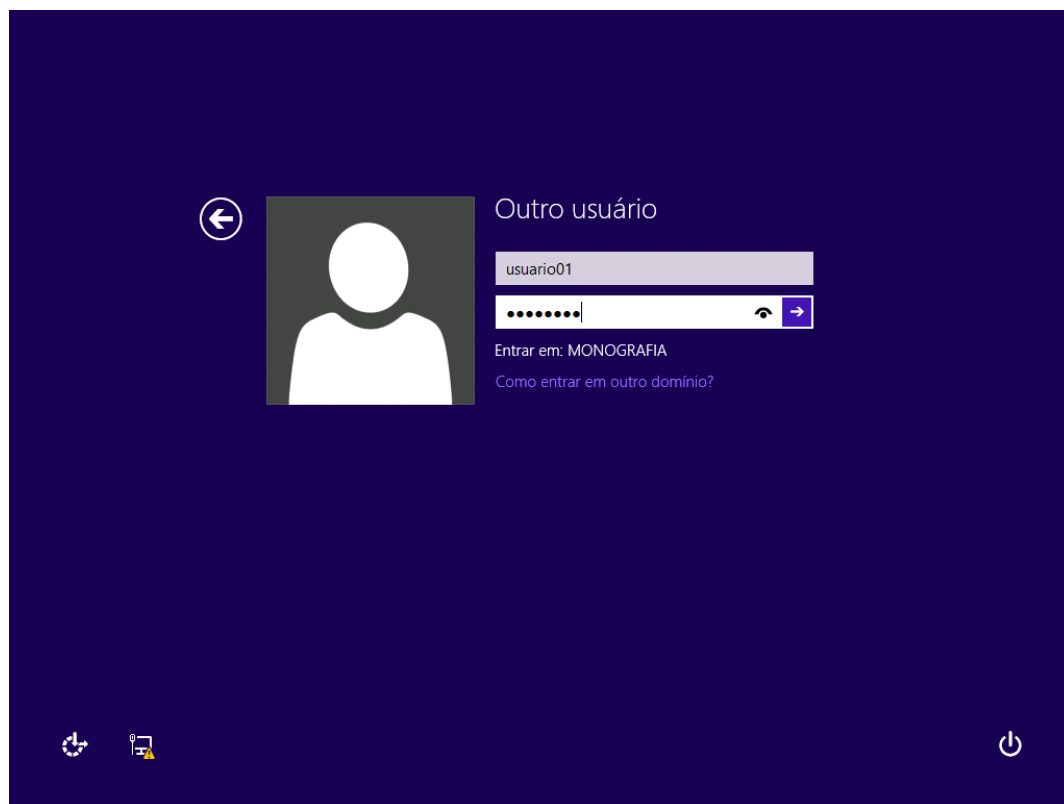
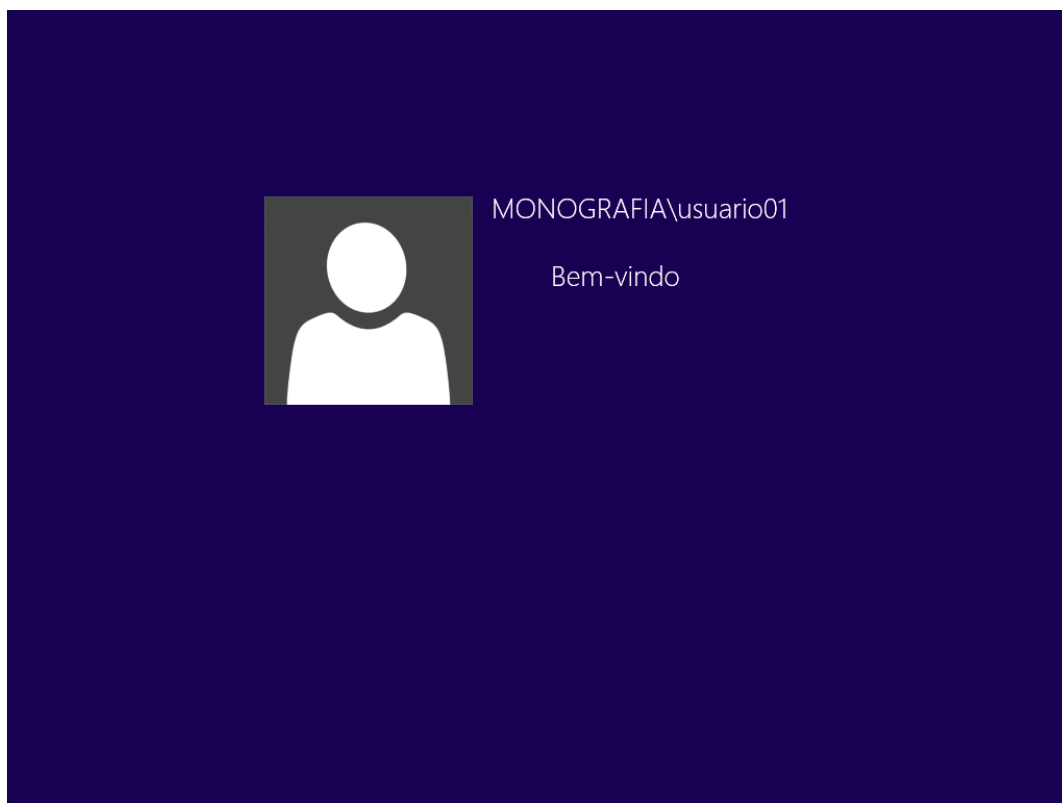


Figura 176 – Boas Vindas ao Domínio



CONCLUSÃO

O estudo permitiu compreender que as duas ferramentas analisadas no trabalho tem suas dificuldades. Durante os estudos alguns fatores puderam ser claramente observados causando grande discrepância entre as duas ferramentas. O fator de acesso a informação e estudos relacionados é muito diferente entre as duas ferramentas, para instalar e configurar o Active Directory encontram-se na internet muitos materiais dispostos, desde fóruns com discussões sobre o assunto até ao próprio site da Microsoft mostrando passo a passo para instalar e configurar a ferramenta. O OpenLDAP tem bastante informação na *web* mas na sua grande parte em fóruns. A maioria dos sites que chamam de *sites* oficiais acabam apresentando links para outros sites como se parte do sistema de serviço de diretório oferecido pela OpenLDAP pertencesse a outras marcas e programas. Existe uma grande dificuldade em conseguir materiais específicos com o passo a passo completo, pois as distribuições Linux dependem de uma série de programas que são pré-requisitos para que o sistema funcione, além de haverem divergências entre esses pré-requisitos e entre as distribuições.

Por um fator de complexidade na instalação e configuração, pode-se observar que as duas ferramentas também divergem muito. O Active Directory oferece uma interface gráfica interativa com o administrador do servidor. A cada clique dado existe uma sugestão do próximo clique. Cada função configurada no servidor é configurada através de WIZARD que orienta o administrador e questiona quanto a serviços completos. O OpenLDAP não tem uma interface gráfica amigável, apesar de poder ser instalada, essa interface não oferece uma interação com usuário. Se o administrador do servidor não tiver o conhecimento necessário a nível de comando estruturado, tiver noção de redes básica, souber fazer configuração de partições de disco, virtualização de máquinas, entre outros conhecimentos básicos, o sistema não tem aplicabilidade.

Analisando o fator de eficácia, tanto o Active Directory como o OpenLDAP atendem ao que pode ser considerado básico em uma segurança de redes, a autenticação de usuários por meio de senha.

Desta forma é observado que a ferramenta de administração de serviços de diretório da Microsoft é a melhor opção para administração de redes com segurança e suporte na visão do autor deste trabalho. Porém para pequenas redes, o OpenLDAP, por ser uma ferramenta grátis, pode ser uma opção, exigindo apenas que o administrador da rede tenha o conhecimento demandado.

REFERÊNCIAS

BUTCHER, M. **Mastering OpenLDAP: Configuring, Securing and Integrating Directory Services**. Birmingham, UK: Packet Publishing Ltd, 2007.

CARTER, G.; TS, J.; ECKSTEIN, R. Using Samba. Unites States os America: O'Reilly Media, Inc, 2007.

FOROUZAN, B. A.; FEGAN, S. C. **Protocolo TCP IP**. Porto Alegre: Mc Grall Hill, 2008.

IETF **RFC 2251**. Disponível em: <<http://www.ietf.org/rfc/rfc2251.txt>>. Acesso em 14/11/2013.

JACKIEWICZ, T. **Deploying OpenLDAP**. New York, USA: Apress, 2005.

MARINHO, R. **O que é o Active Directory**. Disponível em: <<http://www.linhadecodigo.com.br/artigo/2422/o-que-e-o-active-directory.aspx>>. Acesso em 02/09/2013.

MICROSOFT CORP. **Configuring and Troubleshooting Windows Server 2008 Active Diretory Domain Services**. Brazil: Cargraphics Gráfica e Editora Ltda, 2011

RIBEIRO, A. M.; COSTA, C. M.; MENEGUETTI, E.; GRANVILLE, L. Z. **ANAIS**. Porto Alegre: Evangraf Ltda, 2004, p. 91 – 94.

RICHARDS, J.; ALLEN, R.; LOWE-NORRIS, A. G. **Active Directory, Third Edition**. United States of America: O'Reilly Media, Inc, 2006.

SHERESH, B.; SHERESH, D. **Understanding Directory Services**. United States of America: SAMS, 2002, p. 299 – 302.